Schémas pratiques pour la diffusion (sécurisée) sur les canaux sans fils

Zeina Mheich

▶ **To cite this version:**

Zeina Mheich. Schémas pratiques pour la diffusion (sécurisée) sur les canaux sans fils. Autre [cond-mat.other]. Université Paris Sud - Paris XI, 2014. Français. NNT : 2014PA112095 . tel-01059512

HAL Id: tel-01059512
https://theses.hal.science/tel-01059512

Submitted on 1 Sep 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITE PARIS-SUD

ÉCOLE DOCTORALE : STITS
Laboratoire des signaux et systèmes (LSS)

DISCIPLINE : Physique

THÈSE DE DOCTORAT

soutenue le 18/06/2014

par

Zeina MHEICH

Schémas pratiques pour la diffusion (sécurisée) sur les canaux sans fils

Directeur de thèse :	Pierre DUHAMEL	Directeur de recherche CNRS (LSS)
Co-directeur de thèse :	Florence ALBERGE	Maitre de conférences (LSS)

Composition du jury :

Président du jury :	Philippe LOUBATON	Professeur (Université de Marne la Vallée)
Rapporteurs :	Inbar FIJALKOW	Professeur (ENSEA)
	Ghaya REKAYA-BEN OTHMAN	Professeur (Télécom ParisTech)
Examinateurs :	Matthieu BLOCH	Assistant Professor (Georgia Institute of Technology)
	Claudio WEIDMANN	Maitre de conférences (Université Cergy-Pontoise)

Résumé

Dans cette thèse, on s'est intéressé à l'étude des canaux de diffusion avec des contraintes de transmission pratiques. Tout d'abord, on a étudié l'impact de la contrainte pratique de l'utilisation d'un alphabet fini à l'entrée du canal de diffusion Gaussien avec deux utilisateurs. Deux modèles de canaux de diffusion sont considérés lorsqu'il y a, en plus d'un message commun pour les deux utilisateurs, (i) un message privé pour l'un des deux utilisateurs sans contrainte de sécurité (ii) un message confidentiel pour l'un des deux utilisateurs qui doit être totalement caché de l'autre utilisateur. On a présenté plusieurs stratégies de diffusion distinguées par leur complexité d'implémentation. Plus précisément, on a étudié les régions des débits atteignables en utilisant le partage de temps, la superposition de modulation et le codage par superposition. Pour la superposition de modulation et le cas général du codage par superposition, les régions des débits atteignables maximales sont obtenues en maximisant par rapport aux positions des symboles dans la constellation et la distribution de probabilité jointe. On a étudié le compromis entre la complexité d'implémentation des stratégies de transmission et leurs efficacités en termes de gains en débits atteignables. On a étudié aussi l'impact de la contrainte de sécurité sur la communication en comparant les débits atteignables avec et sans cette contrainte. Enfin, on a étudié les performances du système avec des schémas d'accusés de réception hybrides (HARQ) pour un canal à écoute à évanouissement par blocs lorsque l'émetteur n'a pas une information parfaite sur l'état instantané du canal mais connait seulement les statistiques. On a considéré un schéma adaptatif pour la communication sécurisée en utilisant des canaux de retour à niveaux multiples vers l'émetteur pour changer la longueur des sous mots de code à chaque retransmission afin que le débit utile secret soit maximisé sous des contraintes d'*outages*.

Remerciements

Mes remerciements vont tout d'abord à mon directeur de thèse Pierre Duhamel qui a accepté de me choisir en tant que doctorant. Je lui remercie pour sa disponibilité, ses compétences et son encouragement pour mener à bien ces travaux. J'en profite ici pour lui exprimer toute ma profonde gratitude. Je remercie également ma co-directrice de thèse Florence Alberge pour m'avoir assuré les bonnes conditions pour le meilleur déroulement de la thèse et pour son encouragement permanent.

J'adresse également mes remerciements aux membres de Jury qui m'ont fait l'honneur de valider ce travail. Merci à Prof. Inbar Fijalkow et Prof. Ghaya Rekaya-Ben Othman pour avoir eu la volonté de relire et de commenter mon manuscrit. Je tiens à remercier également Prof. Philippe Loubaton, Prof. Claudio Weidmann et Prof. Matthieu Bloch d'avoir accepté de faire partie de mon Jury de thèse en tant qu'examinateurs.

Je voulais ensuite remercier les autres personnes avec qui j'ai eu l'occasion de travailler pendant la thèse, et tout d'abord Prof., Leszek Szczecinski pour son excellent accueil lors de mon séjour à l'INRS au Canada. Je remercie également Dr. Mael Le Treust pour les discussions en théorie de l'information qui m'ont permis de comprendre beaucoup de choses et aussi pour son soutien au cours de la thèse. Je remercie aussi Dr. Marie-Line Alberi-Morel, qui m'avait encadré pendant mon stage de M2 et qui a représenté un soutien important tout au long de mon stage.

Je tiens également à remercier tous mes professeurs de l'université libanaise, faculté de génie, branche 1 et surtout Dr. Rima Hleiss qui m'a encouragé à continuer dans le domaine de la recherche suite au stage de fin d'études que j'ai effectué sous sa direction.

Je tiens également à remercier mes amis à LSS et à Supelec que j'ai rencontrés. Merci à Elsa, François, Benjamin, Leila, Thang, Vineeth, Pierre, Achal, Etienne, Chengfang, Olivier, Diane, Anna, Mathieu, Florian, Jinane, Amina, Safaa, Azary, Sarra, Sabrine, Assia, Mahmoud, Meryem, Maggie, José, Ziad, Nabil, Lana, Amadou, Francesca, Hacheme... Et un grand merci pour mes parents pour leur soutien et leur amour.

Table des matières

Table des figures

Liste des tableaux

Acronymes

- **ACK** : ACKnowledge
- **AWGN** : Additive White Gaussian Noise
- **BICM** : Bit-Interleaved Coded Modulation
- **BPSK** : Binary Phase Shift Keying
- **CSI** : Channel State Information
- **DVB-H** : Digital Video Broadcast to Handhelds
- **DVB-SH** : Digital Video Broadcast services to Handhelds
- **DVB-T** : Digital Video Broadcast for Terrestrial Television
- **HARQ** : Hybrid Automatic Repeat reQuest
- **HM** : Hierarchical Modulation
- **i.i.d.** : independent and identically distributed
- **INR** : INcremental Redundancy
- **LDPC** : Low-Density Parity-Check
- **LTE** : Long Term Evolution
- **MISO** : Multiple Input Single Output
- **MIMO** : Multiple Input Multiple Output
- **NACK** : Negative-ACKnowledge
- **OFDM** : Orthogonal Frequency-Division Multiplexing
- **PAM** : Pulse Amplitude Modulation
- **pdf** : probability density function
- **PàP** : Point-à-Point

– **QAM** : Quadrature Amplitude Modulation
– **QPSK** : Quadrature Phase-shift keying
– **SC** : Superposition Coding
– **SM** : Superposition Modulation
– **RSB** : Rapport Signal sur Bruit
– **TS** : Time Sharing

Chapitre 1

Introduction

1.1 Motivations et objectifs de la thèse

En 1948 Claude E. Shannon a introduit les idées de la théorie de l'information dans son célèbre article "*A Mathematical Theory of Communications*" [3]. Dans son papier, Shannon a formulé un modèle de système de communication point à point, remarquable par sa généralité et sa simplicité, pour lequel il a fourni une théorie complète. On connait maintenant des codes puissants permettant d'approcher les limites données par la théorie de l'information pour un canal point à point. Cependant, ce modèle ne rend pas compte de nombreux aspects importants des systèmes du monde réel.

Au cours des dernières décennies, les réseaux d'information ont connu d'énormes progrès, basés sur la croissance importante dans l'adoption de nouvelles technologies sans fil, des applications et des services [4]... Les utilisateurs souhaitent maintenant par exemple écouter ou télécharger des services orientés vidéo à travers des réseaux partagés, ce qui nécessite d'exploiter pleinement leurs ressources spectrales déjà restreintes. Les techniques optimales de partage des ressources radio sont hautement souhaitables pour les opérateurs mobiles afin de permettre à tous ces appareils d'être connectés sur les réseaux sans fil, avec une qualité de service prédéfinie garantie. En raison de l'augmentation de l'intérêt des applications de la théorie de l'information, la recherche actuelle est motivée par la conception des systèmes de communication multi-utilisateurs, les réseaux

informatiques, les communications coopératives, des modèles de réseaux avec contraintes de sécurité...

Dans cette thèse, nous nous concentrons sur l'étude des modèles de système de diffusion sur les canaux sans fils. Le canal de diffusion est défini en théorie de l'information comme un canal de communication dans lequel il y a un émetteur et plusieurs récepteurs [5]. Les transmissions radio et TV, un conférencier dans une classe sont des exemples de diffusion [6].

Puisque la sécurisation des systèmes et des réseaux sans fil est devenue une préoccupation importante avec la croissance des communications sans fil, on va étudier aussi des modèles de canaux de diffusion avec contrainte de sécurité. Par rapport aux réseaux câblés, les réseaux sans fil ajoutent un niveau supplémentaire de complexité, lorsqu'il s'agit d'assurer la sécurité des communications. La nature de la diffusion des communications sans fil rend les données plus sensibles à l'écoute. Alors que les réseaux câblés envoient des signaux électriques ou des impulsions de lumière par câble, les signaux radio sans fil se propagent dans l'air et sont naturellement plus faciles à intercepter. Traditionnellement, la sécurité est mise en œuvre dans les systèmes de communication en utilisant des techniques cryptographiques dans les couches supérieures de la pile du protocole. Ces techniques sont basées sur l'hypothèse d'une puissance de calcul limitée chez l'espion. Récemment, la sécurité au niveau de la couche physique du point de vue de la théorie de l'information, est devenue un sujet de grand intérêt. Cette technique exploite le caractère aléatoire des canaux sans fil et ne suppose aucune restriction de calcul chez l'espion. Dans [7], Wyner a introduit le canal à écoute ("*wiretap channel*") où l'émetteur veut envoyer un message confidentiel à un récepteur légitime en présence d'un espion. Wyner a étudié le canal à écoute où le signal reçu par l'espion est une version dégradée du signal reçu par le récepteur légitime. Le niveau d'ignorance chez l'espion relativement au message confidentiel est mesuré par le taux d'ambiguïté ("*equivocation rate*"). Wyner a démontré que la communication sécurisée est possible sans partager une clé secrète et a déterminé la capacité secrète du canal à écoute dégradé sans mémoire. La capacité secrète est le débit atteignable maximal pour communiquer d'une manière fiable avec la destination

sans que l'espion soit capable d'obtenir une information sur le signal émis. Dans [8], la capacité secrète est donnée pour le canal à écoute Gaussien. Csiszar et Korner ont étudié dans [9] un modèle plus général que le canal à écoute, appelé canal de diffusion avec message confidentiel où les canaux ne respectent pas nécessairement une relation de dégradation. Dans ce modèle, il y a un message commun pour les deux récepteurs en plus du message confidentiel pour l'un des récepteurs. Plus récemment, le modèle de canal à évanouissement a été introduit dans le modèle de la transmission secrète [10],[11],[12] et les canaux à écoute Gaussien MIMO et MISO sont revisités dans [13] et [14] respectivement. Des études récentes ont considérés la communication multi-utilisateurs avec des messages confidentiels comme les canaux à accès multiples avec messages confidentiels [15], [16], les canaux à écoute à accès multiples [17], [18] et les canaux d'interférence avec messages confidentiels [19], [20].

Cependant, la plupart des résultats classiques sur les limites théoriques de la communication et les schémas qui permettent de les atteindre ne sont pas toujours réalisables en pratique. La plupart de ces résultats supposent que l'émetteur et le récepteur connaissent parfaitement les paramètres du canal ce qui est peu réaliste. Dans le cas des canaux de diffusions Gaussiens à deux utilisateurs que nous allons traiter dans cette thèse, Cover a montré que l'on peut faire mieux en terme de débits que le partage de temps pour servir les utilisateurs, et ce en utilisant le codage par superposition [5]. Cover et Bergmans ont démontré que le codage par superposition atteint la limite théorique de la région de capacité pour un canal de diffusion Gaussien en utilisant un alphabet d'entrée Gaussien [5], [21], [22]. Cependant, dans les systèmes de transmission réels, l'entrée du canal est limitée à un alphabet de taille finie et les symboles transmis appartiennent à des constellations telle que M-PAM, M-QAM,... La modulation hiérarchique est un exemple pratique de codage par superposition. Elle a été incluse dans plusieurs standards y compris le DVB-T/H/SH [23],[24] pour la transmission des médias numériques "*scalable*" pour la télévision numérique mobile [25]. Cette technique permet la transmission de deux flux de services indépendants sur une même bande avec différentes qualités de transmission en utilisant des constellations dont les symboles sont espacés d'une façon non-uniforme

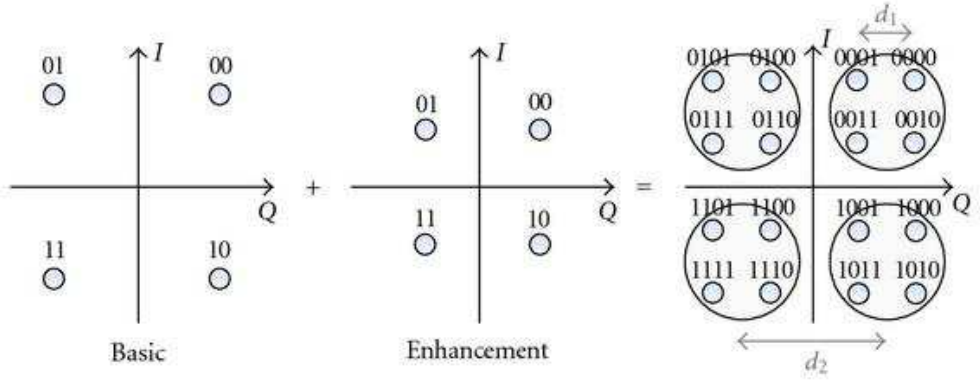

FIGURE 1.1 – Constellation d'une modulation hiérarchique 16-QAM [2].

et utilisés avec la même probabilité. Dans la figure 1.1, la constellation d'une modulation hiérarchique 16-QAM est représentée. Deux flux de donnés indépendants coexistent avec différentes exigences de sensibilité au canal. Dans cet exemple, le flux de haute priorité ("*high priority stream*" ou "*basic stream*") utilise une modulation QPSK et il est destiné à couvrir la zone de service entière. Le flux de basse priorité ("*low priority stream*" ou "*enhancement stream*") nécessite de démoduler la constellation comme une 16-QAM et fournit un service supplémentaire via les deux bits additionnels.

La restriction imposée par les systèmes pratiques d'utiliser des constellations finies et des symboles équiprobables réduit les débits atteignables et conduit à un écart avec la région de capacité atteinte avec des alphabets d'entrée gaussiens pour le canal de diffusion gaussien. Cet écart peut être réduit à l'aide d'une technique appelée "mise en forme de la constellation" ("*constellation shaping*"). En fait, la plupart des résultats concernant la mise en forme de la constellation ne considèrent que les systèmes de communication point-à-point [26]. Puis, ce concept a été adapté à des techniques de modulation et de codage moderne comme par exemple les turbocodes, les codes LDPC et les techniques BICM [27]-[36]. La région de débits atteignables pour un canal de diffusion Gaussien à deux utilisateurs est donnée dans [37] pour un cas particulier lorsque les symboles de la constellation sont utilisés avec la même probabilité et lorsque la superposition du signal

modulé est utilisée en tant que stratégie de transmission.

Dans cette thèse, on va considérer aussi le modèle du canal de diffusion avec contrainte de sécurité. Dans la littérature, plusieurs travaux ont été faits sur l'étude du débit secret atteignable avec alphabet fini pour le canal à écoute seulement. Le canal à écoute est un cas particulier du modèle du canal de diffusion avec message confidentiel étudié dans cette thèse, où l'émetteur a aussi un message commun pour les utilisateurs. Dans [38] et [39], les auteurs considèrent le débit secret atteignable pour le canal à écoute. Les courbes des débits secrets atteignables en utilisant des constellations finies en fonction du *RSB* et pour une variance de bruit fixée du canal de l'espion possèdent un maximum global en un point interne. Cela vient en contraste avec ce qui est connu dans le cas d'une entrée Gaussienne, où la courbe de la région de capacité secrète est une fonction bornée, croissante du *RSB*. La référence [40] étudie le débit secret du canal à écoute Gaussien en utilisant des M-PAM standards. Les auteurs fournissent les conditions nécessaires pour la puissance moyenne et la distribution des symboles du M-PAM à la fois afin de maximiser le débit secret et les spécialisent pour les régimes asymptotiques à faible puissance et à haute puissance ("*low-power and high-power regimes*"). Les références [41] et [42] étudient l'effet des constellations finies sur le débit secret atteignable pour les canaux à écoute multi-antennes. Dans [43], les auteurs étudient l'allocation de puissance et la conception du bruit artificiel pour les canaux OFDM à écoute avec des alphabets d'entrée finis.

L'objectif de cette thèse est d'étudier les limites de la communication fiable (et sécurisée) avec des contraintes de transmission pratiques. Le chapitre 3 étudie l'impact de la contrainte d'alphabet d'entrée fini, avec et sans contrainte de sécurité pour un canal de diffusion Gaussien. Pour cela on va considérer deux types de canaux de diffusion Gaussien : (i) un cas où l'émetteur envoie un message commun pour deux utilisateurs et un message privé pour l'un des deux utilisateurs (ii) un autre cas où l'émetteur veut envoyer un message commun pour deux utilisateurs et un message confidentiel pour un récepteur légitime. On va supposer que les symboles à l'entrée du canal appartiennent à des constellations finies de type M-PAM. Les positions des symboles,

dans ce chapitre, peuvent prendre des valeurs arbitraires et ne sont pas nécessairement proportionnelles à celles de la constellation M-PAM standard comme dans [40]. Les débits atteignables seront étudiés pour plusieurs stratégies de transmission (incluant la modulation hiérarchique) ayant des complexités d'implémentation différentes. Le but sera d'évaluer la perte en terme de débits en utilisant les stratégies simples et d'identifier les situations dans lesquelles les schémas complexes (non-standard) conduisent à des améliorations significatives. On comparera aussi les résultats obtenus pour les deux types de canaux de diffusion considérés (sans et avec contrainte de sécurité) et on analysera l'effet de la contrainte de sécurité sur les débits atteignables. Dans le chapitre 3, l'état instantané des canaux est supposé d'être connu par l'émetteur et les récepteurs.

Dans le chapitre 4, on considère le canal à écoute à évanouissement par blocs dans lequel l'émetteur n'a pas une information sur l'état instantané du canal "*CSI (channel state information)*", mais connait seulement les statistiques. Cette hypothèse est très intéressante pour beaucoup de systèmes de communications pratiques. L'émetteur veut envoyer un message confidentiel à un récepteur légitime en présence d'un espion. L'objectif dans ce chapitre est l'étude des performances du système avec des schémas d'accusés de réception hybrides (HARQ). Les protocoles HARQ sont une classe spéciale des schémas de codage qui combinent à la fois un codage canal efficace avec les protocoles de transmission pour améliorer la fiabilité des liens de communication. On va considérer les protocoles HARQ avec un nombre limité de tentatives de transmission lorsque la communication sécurisée et sans erreur ne peut être garantie. On va considérer aussi un schéma puissant de HARQ appelé "redondance incrémentale" (*incremental redundancy*) où plusieurs ensembles de bits codés sont générés et utilisés dans les retransmissions, représentant chacun le même bloc de données. Le défi de ce problème est que le codeur a besoin de fournir une redondance suffisante pour que le récepteur légitime décode correctement le message ; cependant, trop de redondance peut aider l'espion. En effet, la retransmission est une manière efficace pour améliorer la fiabilité mais elle peut aussi compromettre la confidentialité. Pour pallier à cela, nous considérons conjointement le codage canal, le codage secret et les protocoles de retransmission. Puisque l'émetteur ne

connait pas l'état instantané du canal, il ne peut pas adapter les débits aux conditions instantanés du canal. Dans ce travail, on suppose qu'il existe des canaux de retour à niveaux multiples du récepteur légitime et de l'espion à la fois vers l'émetteur. Par suite, l'émetteur peut adapter la longueur des sous-mots de code à chaque retransmission en utilisant les canaux de retour afin de maximiser le débit utile secret sous contraintes d'*outages* [44],[45],[46],[47] qui nous permet de prendre en compte la qualité de service requise. L'objectif sera de comparer le schéma adaptatif à débit variable dans chaque retransmission au schéma non-adaptatif à débit fixe dans [48].

1.2 Structure du manuscrit et contributions

Dans ce manuscrit, on ne présente que les résultats principaux des travaux menés au cours de cette thèse. Le détails des calculs et les analyses plus approfondies des simulations sont présentés dans les annexes. Le manuscrit de thèse est organisé comme suit :

Dans le chapitre 2, on présente les résultats principaux issus de la théorie de l'information portant sur les débits atteignables pour les canaux de diffusion avec et sans contrainte de sécurité. En particulier, pour un canal de diffusion Gaussien avec deux utilisateurs et une contrainte de puissance à l'émetteur, la région de capacité est atteinte en utilisant un alphabet d'entrée Gaussien.

Dans le chapitre 3, on étudie les débits atteignables pour le canal de diffusion Gaussien avec deux utilisateurs et une contrainte de puissance en utilisant des alphabets d'entrée finis. On considère deux types de canaux de diffusion avec : (i) un message commun pour les deux récepteurs et un message privé pour l'un des deux, (ii) un message commun pour les deux récepteurs et un message confidentiel. On étudie les régions de débits atteignables pour différentes stratégies de transmission : le *time sharing*, la superposition de modulation et le codage par superposition. Pour cela, nous avons conçu un algorithme permettant de maximiser les régions des débits atteignables par rapport aux positions des symboles dans la constellation et par rapport à la distribution de pro-

babilité jointe. Nous ferons aussi une comparaison entre les deux types des canaux de diffusion considérés en terme des débits atteignables.

Le chapitre 4 étudie un schéma "adaptatif" pour la communication sécurisée basée sur les protocoles HARQ pour les canaux à écoute à évanouissement lorsque l'émetteur n'a pas une connaissance parfaite de l'état instantané du canal. L'émetteur connait seulement les statistiques du canal et peut recevoir les états passés du canal par l'intermédiaire des canaux de retour du récepteur légitime et de l'espion. En utilisant les canaux de retour, l'émetteur peut adapter la longueur des sous-mots de code afin de maximiser le débit utile secret. La méthode utilisée pour optimiser le débit utile secret pour la transmission avec des contraintes d'*outages* est basée sur la programmation dynamique. On compare aussi le schéma adaptatif à débit variable dans chaque retransmission au schéma non-adaptatif à débit fixe existant dans la littérature [48].

Enfin, le chapitre 5 résume les principales conclusions de nos travaux tout en posant les perspectives.

1.3 Publications

Les travaux de recherche menés au cours des trois années de thèse ont conduit aux publications suivantes :

1.3.1 Revues internationales

- [49] Zeina Mheich, Marie-Line Alberi Morel, and Pierre Duhamel. *Optimization of unicast services transmission for broadcast channels in practical situations*. Bell Labs Technical Journal, 17(1) :5-23, 2012.
- [1] Zeina Mheich, Florence Alberge, and Pierre Duhamel. *Achievable rates optimization for broadcast channels using finite size constellations under transmission constraints*. EURASIP Journal on Wireless Communications and Networking, 2013(1) :254, 2013.

1.3.2 Congrès internationaux avec comité de lecture et actes

- [50] Zeina Mheich, Pierre Duhamel, Leszek Szczecinski, and Marie-Line Alberi Morel. *Constellation shaping for broadcast channels in practical situations.* Proceedings of the 19th European Signal Processing Conference (EUSIPCO 2011), Barcelona, 29 Aug-2 Sept. 2011.
- [51] Zeina Mheich, Florence Alberge, and Pierre Duhamel. *On the efficiency of transmission strategies for broadcast channels using finite size constellations.* Proceedings of the 21st European Signal Processing Conference (EUSIPCO 2013), Marrakech, 9-13 Sept. 2013.
- [52] Zeina Mheich, Florence Alberge, and Pierre Duhamel. *The impact of finite-alphabet input on the secrecy-achievable rates for broadcast channel with confidential message.* IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2014), Florence, 4-9 Mai 2014.

1.3.3 Travaux soumis

- [53] Zeina Mheich, Maël Le Treust, Florence Alberge, Pierre Duhamel and Leszek Szczecinski. *Rate-adaptive secure HARQ protocol for block-fading channels.* Soumis à 22nd European Signal Processing Conference (EUSIPCO 2014), Mars 2014.
- [54] Zeina Mheich, Florence Alberge, and Pierre Duhamel. *Secrecy-achievable rates for the broadcast channel with confidential message and finite constellation inputs.* Soumis à IEEE transactions on communications, Avril 2014.

Chapitre 2

Canaux de diffusion

Sommaire

2.1 Introduction

L'objectif de ce chapitre est de présenter quelques résultats en théorie de l'information liés au cadre de cette thèse. On va considérer deux types de canaux de diffusion. Dans la première partie, on s'intéresse à étudier le canal de diffusion avec deux utilisateurs lorsque l'émetteur a un message commun pour les deux utilisateurs et un message privé dédié à l'utilisateur 1. Dans la deuxième partie, on suppose qu'il y a une contrainte de sécurité

sur le message vers l'utilisateur 1 et on étudie le canal de diffusion où l'émetteur a un message commun pour les deux utilisateurs et un message confidentiel pour l'utilisateur 1. Dans tout le document, les variables aléatoires sont en majuscules, leurs réalisations sont en minuscules.

2.2 Canaux de diffusion avec un message commun et un message privé

2.2.1 Canal de diffusion dégradé

Un canal de diffusion est un canal de communication dans lequel il y a un émetteur et deux ou plusieurs récepteurs. Un canal de diffusion avec deux récepteurs (ou utilisateurs) est composé d'un alphabet d'entrée $\mathcal{X}$, de deux alphabets de sortie $\mathcal{Y}_1$ (utilisateur 1), $\mathcal{Y}_2$ (utilisateur 2) et d'une fonction de probabilité de transition $p(y_1, y_2|x)$. Soient X, Y_1 et Y_2 des variables aléatoires représentant l'entrée et les sorties du canal de diffusion. Le canal de diffusion est dit "sans-mémoire" si $p(y_1^n, y_2^n|x^n) = \prod_{i=1}^{n} p(y_{1i}, y_{2i}|x_i)$. La figure 2.1 représente le canal de diffusion avec deux utilisateurs et deux messages indépendants W_0 et W_1 pour lequel W_1 désigne le message privé pour l'utilisateur 1 seulement et W_0 est le message commun pour les deux récepteurs. Un code $(2^{nR_0}, 2^{nR_1}, n)$ pour un canal de diffusion est déterminé par les éléments suivants :

- Deux ensembles de messages $\mathcal{W}_0 = \{1, .., 2^{nR_0}\}$ et $\mathcal{W}_1 = \{1, .., 2^{nR_1}\}$. Les messages W_0 et W_1 sont uniformément distribués sur $\mathcal{W}_0$ et $\mathcal{W}_1$ respectivement.
- Un codeur qui associe une paire de messages $(w_0, w_1) \in (\mathcal{W}_0, \mathcal{W}_1)$ à un mot de code x^n.
- Deux décodeurs : le premier chez le récepteur 1 qui associe une séquence reçue $y_1^n \in \mathcal{Y}_1^n$ à une paire de messages $(\hat{w}_0, \hat{w}_1)$ ou à un message d'erreur e et le deuxième chez le récepteur 2 qui associe une séquence reçue $y_2^n \in \mathcal{Y}_2^n$ à un message $\tilde{w}_0$ ou à un message d'erreur e.

La probabilité d'erreur moyenne $P_e^{(n)}$, mesurant le niveau de fiabilité, est $P_e^{(n)} = \frac{1}{2^{nR_0}2^{nR_1}} \cdot \sum_{w_0=1}^{nR_0} \sum_{w_1=1}^{nR_1} \Pr\{(\hat{w}_0, \hat{w}_1) \neq (w_0, w_1) \text{ or } \tilde{w}_0 \neq w_0\}$.

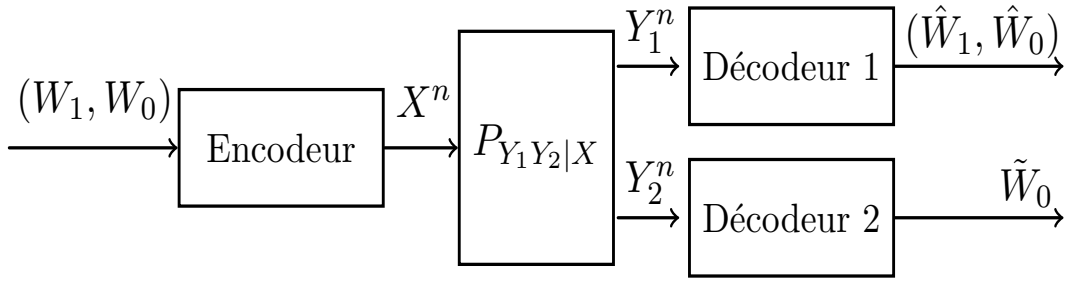

FIGURE 2.1 – Canal de diffusion avec deux récepteurs

Définition 1 *Une paire de débits (R_0, R_1) est dite atteignable pour le canal de diffusion s'il existe une séquence de codes $(2^{nR_0}, 2^{nR_1}, n)$ avec $P_e^{(n)} \to 0$ lorsque $n \to \infty$.*

Définition 2 *La région de capacité du canal de diffusion est la fermeture de l'ensemble des débits atteignables.*

La région de capacité du canal de diffusion n'est pas connue en général. Cependant, la région de capacité est connue pour les canaux de diffusion dits "dégradés".

Définition 3 *Un canal de diffusion est dit physiquement dégradé si $p(y_1, y_2|x) = p(y_1|x)p(y_2|y_1)$. ($X \to Y_1 \to Y_2$ est une chaine de Markov)*

Définition 4 *Un canal de diffusion est dit stochastiquement dégradé s'il existe une variable aléatoire qui a la même densité de probabilité conditionnelle que Y_1 sachant X telle que $X \to \tilde{Y_1} \to Y_2$ forme une chaine de Markov.*

La région de capacité du canal de diffusion stochastiquement dégradé est la même que celle du canal de diffusion physiquement dégradé correspondant. On considère maintenant le canal de diffusion dégradé dans lequel l'émetteur envoie W_0 et W_1 avec des débits R_0 et R_1 respectivement. On rappelle que l'utilisateur 1 atteint le débit $R_0 + R_1$, puisque W_0 est un message commun alors que l'utilisateur 2 atteint seulement R_0.

Théorème 1 *La région de capacité pour le canal de diffusion dégradé $X \to Y_1 \to Y_2$ est l'enveloppe convexe de l'ensemble de toutes les paires (R_0, R_1) satisfaisant*

$$R_1 \leq I(X; Y_1|U) \tag{2.1}$$

$$R_0 \leq I(U;Y_2) \tag{2.2}$$

pour certaine distribution jointe $P_{UXY_1Y_2} = P_{UX} \cdot P_{Y_1|X} \cdot P_{Y_2|X}$ *sur* $\mathcal{U} \times \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2$. $P_{Y_1|X}$ *et* $P_{Y_2|X}$ *sont les fonctions densité de probabilités conditionnelles qui dépendent du modèle du canal.* P_{UX} *est la distribution de probabilité jointe de* U *et* X*, où la cardinalité de* $\mathcal{U}$ *est bornée par* $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$.

La région de capacité pour le canal de diffusion dégradé est atteignable en utilisant le codage par superposition. Le codage par superposition apparait dans plusieurs contextes de la théorie de l'information et il est étroitement lié au codage multi-couches [55], [56]. L'idée du codage par superposition est résumée dans ce qui suit. La variable aléatoire auxiliaire U sert de centre aux nuages distingué par les deux récepteurs 1 et 2. Chaque nuage est constitué de 2^{nR_1} mots de codes X^n distingués par le récepteur 1. Le récepteur 2 peut distinguer seulement les nuages alors que le récepteur 1 peut voir aussi les mots de codes individuels dans les nuages. La preuve formelle de l'atteignabilité de la région de capacité utilise un argument de codage aléatoire "*random coding*" et contient les étapes suivantes. On fixe tout d'abord $p(u)$ et $p(x|u)$. La génération du "*codebook*" est faite d'une manière aléatoire en générant 2^{nR_0} mots de codes indépendants de longueur n, $u^n(w_0)$, $w_0 \in \{1, 2, .., 2^{nR_0}\}$, selon $\prod_{i=1}^{n} p(u_i)$. Pour chaque mot de code $u^n(w_0)$, sont générés 2^{nR_1} mots de codes indépendants $x^n(w_0, w_1)$ selon $\prod_{i=1}^{n} p(x_i|u_i(w_0))$. Ici, $u^n(w_0)$ joue le rôle du centre de nuage compréhensible par les deux récepteurs à la fois, alors que $x^n(w_0, w_1)$ est le $w_1^{\text{ème}}$ mot de code satellite ("*satellite codeword*") dans le $w_0^{\text{ème}}$ nuage. Le codage est fait de la manière suivante : pour transmettre la paire (W_0, W_1), le mot de code $x^n(W_0, W_1)$ est envoyé. Le décodage est fait en utilisant la méthode des séquences typiques [57].

L'atteignablité de la région dans le Théorème 1 pour le canal de diffusion dégradé a été établi par Bergmans [21]. Environ un an plus tard, l'optimalité des ensembles des débits atteignables (dans le Théorème 1) pour le canal de diffusion dégradé a été établi par Bergmans [22] et Gallager [58].

2.2.2 Canal de diffusion Gaussien

Considérons maintenant le canal de diffusion Gaussien avec deux utilisateurs. On suppose qu'il existe une contrainte de puissance P au niveau de l'émetteur : $\mathbb{E}[X^2] \leq P$. On suppose, sans perte de généralité, que Y_1 est moins bruyant que Y_2. On peut facilement montrer que le canal de diffusion Gaussien est équivalent à un canal dégradé, puisque le canal peut être représenté comme dans la figure 2.2 :

$$Y_1 = X + Z_1 \tag{2.3}$$

$$Y_2 = X + Z_2 = Y_1 + Z_2' \tag{2.4}$$

où $Z_1 \sim \mathcal{N}(0, \sigma_1^2)$, $Z_2 \sim \mathcal{N}(0, \sigma_2^2)$, $Z_2' \sim \mathcal{N}(0, \sigma_2^2 - \sigma_1^2)$ et Z_1, Z_2' sont indépendants. Le rapport signal sur bruit reçu pour chaque utilisateur est $RSB_i = \frac{P}{\sigma_i^2}$, où $RSB_1 > RSB_2$ et $N_i = \sigma_i^2$ est la variance du bruit Z_i.

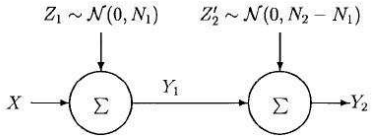

FIGURE 2.2 – Canal de diffusion Gaussien

Théorème 2 *La région de capacité du canal de diffusion Gaussien avec une contrainte de puissance P est donnée par :*

$$R_1 \leq C(\alpha \cdot RSB_1) \tag{2.5}$$

$$R_0 \leq C\left(\frac{(1-\alpha) \cdot RSB_2}{\alpha \cdot RSB_2 + 1}\right) \tag{2.6}$$

pour $\alpha \in [0, 1]$, où $C(x) = \frac{1}{2} \cdot \log_2(1 + x)$.

Cette région est atteignable en utilisant le schéma de codage décrit dans [5]. la méthodologie est la suivante. On choisit 2^{nR_0} mots de codes Gaussiens $u^n(i)$ indépendants et identiquement distribués (i.i.d.) $\sim \mathcal{N}(0, (1-\alpha)P)$. Pour chacun de ces mots de codes $u^n(i)$, on génère 2^{nR_1} mots de codes Gaussien satellites $v^n(j)$ de puissance αP. Les mots de codes $x^n(i, j)$ sont obtenus par $x^n(i, j) = u^n(i) + v^n(j)$.

2.3 Canaux de diffusion avec un message confidentiel

Dans cette section, on résume quelques résultats théoriques sur les débits atteignables pour le canal de diffusion avec message confidentiel.

2.3.1 Canaux de diffusion avec message confidentiel

Un canal de diffusion avec message confidentiel est un canal de diffusion avec deux récepteurs pour lesquels un émetteur tente d'envoyer deux messages simultanément : un message commun w_0 pour les deux récepteurs et un message confidentiel w_1 pour le récepteur 1 [9]. La différence entre un code $(2^{nR_0}, 2^{nR_1}, n)$ pour le canal de diffusion avec message confidentiel et celui pour le canal de diffusion sans contrainte de sécurité dans le paragraphe 2.2.1, est l'utilisation d'un codeur randomisé ("*randomized encoder*") pour assurer la sécurité. Le niveau de confidentialité du message confidentiel W_1 chez l'espion est mesuré par le taux d' équivoque ("*equivocation rate*"). Le niveau de fiabilité est mesuré par la probabilité d'erreur moyenne $P_e^{(n)}$ définie dans le paragraphe 2.2.1.

Définition 5 *Le triplet débit-équivoque (R_0, R_1, R_e) est atteignable s'il existe une séquence de codes $(2^{nR_0}, 2^{nR_1}, n)$ avec $P_e^{(n)} \to 0$ quand $n \to \infty$ et avec un taux d'équivoque satisfaisant $R_e \leq \liminf_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n)$.*

Tout au long de ce travail, on se concentre sur le cas où la "confidentialité parfaite" ("*perfect secrecy*") est atteinte : $R_1 = R_e$, *i.e.* les messages confidentiels transmis sont entièrement cachés de l'espion.

Définition 6 *La région de capacité secrète est l'ensemble de toutes les paires de débits (R_0, R_1) telles que $(R_0, R_1, R_e = R_1)$ est atteignable.*

Théorème 3 *La région de capacité secrète, donnée dans [9], est l'enveloppe convexe de l'ensemble de toutes les paires (R_0, R_1) satisfaisant :*

$$0 \leq R_1 \leq I(V; Y_1|U) - I(V; Y_2|U) \tag{2.7}$$

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} \tag{2.8}$$

pour une certaine distribution $P_{UVXY_1Y_2} = P_U \cdot P_{V|U} \cdot P_{X|V} \cdot P_{Y_1Y_2|X}$ *sur* $\mathcal{U} \times \mathcal{V} \times \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2$ *où* U *et* V *sont des variables aléatoires auxiliaires satisfaisant* $U \leftrightarrow V \leftrightarrow X \leftrightarrow Y_1Y_2$. *Les cardinalités des ensembles* $\mathcal{U}$ *et* $\mathcal{V}$ *peuvent être limitées à* $|\mathcal{U}| \leq |\mathcal{X}| + 3$ *et* $|\mathcal{V}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$.

U sert comme un centre de nuage distingué par les deux récepteurs. En d'autre termes, elle porte l'information commune (même interprétation que dans le paragraphe 2.2.1). V est une variable aléatoire auxiliaire pour une randomisation additionnelle chez l'encodeur.

Corollaire 1 *La région de capacité secrète du canal de diffusion dégradé avec message confidentiel* $U \leftrightarrow V \leftrightarrow X \leftrightarrow Y_1 \leftrightarrow Y_2$ *est la fermeture de l'ensemble de toutes les paires* (R_0, R_1) *satisfaisant [11] :*

$$R_1 \leq I(X;Y_1|U) - I(X;Y_2|U) \tag{2.9}$$

$$R_0 \leq I(U;Y_2) \tag{2.10}$$

où la cardinalité de $\mathcal{U}$ *peut être bornée par* $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$.

On constate que $V = X$ dans le cas du canal dégradé. En comparant avec le cas du canal de diffusion dégradé sans contrainte de sécurité (équations (2.1) et (2.2)), il semble que cette contrainte pénalise le débit du message privé vers l'utilisateur 1 en le diminuant d'une quantité $I(X;Y_2|U)$, pour confondre l'espion, comme c'est indiquée dans l'équation 2.9 ; par contre, cela est trompeur car il est possible d'envoyer aussi un message public privé vers l'utilisateur 1 en plus du message confidentiel pour atteindre la région de capacité du canal de diffusion dégradé sans message confidentiel. Dans cette thèse, on se concentre sur l'étude du débit secret pour l'utilisateur 1 et le débit du message commun seulement.

2.3.2 Canal de diffusion Gaussien avec message confidentiel

On considère maintenant le canal de diffusion Gaussien (dégradé) avec message confidentiel. Les sorties du canal sont $Y_i = X + Z_i$ où $i \in [1, 2]$ et $Z_i \sim \mathcal{N}(0, N_i)$. On considère

aussi une contrainte de puissance à l'entrée du canal $\mathbf{E}[X^2] \leq P$.

Théorème 4 *La région de capacité secrète du canal de diffusion Gaussien avec message confidentiel $X \leftrightarrow Y_1 \leftrightarrow Y_2$ est donnée par [11] :*

$$= \bigcup_{\beta \in [0,1]} \left\{ (R_0, R_1) : \begin{array}{l} R_0 \leq C(\frac{(1-\beta)\cdot P}{N_2+\beta \cdot P}) \\ \\ R_1 \leq C(\frac{\beta \cdot P}{N_1}) - C(\frac{\beta \cdot P}{N_2}) \end{array} \right. \tag{2.11}$$

L'atteignabilité de la région de capacité secrète résulte du corollaire précédant et du choix suivant des variables aléatoires : $U \sim \mathcal{N}(0, (1-\beta)\cdot P)$, $X = U + X'$ avec $X' \sim \mathcal{N}(0, \beta \cdot P)$.

2.3.3 Canal à écoute

On passe maintenant à l'étude d'un cas particulier du canal de diffusion avec message confidentiel appelé canal à écoute dans lequel il n'y a pas de message commun ($R_0 = 0$). La capacité secrète du canal à écoute discret et sans mémoire est obtenue en prenant $U = const$ dans le cas du canal de diffusion avec message confidentiel [9]. Par suite, en remplaçant $U = const$ dans le théorème 3, on obtient le corollaire suivant :

Corollaire 2 *La capacité secrète du canal à écoute discret et sans mémoire est :*

$$R_1 = \max_{P_{VX}} I(V;Y_1) - I(V;Y_2) \tag{2.12}$$

Le concept de "dégradation" dans les canaux de diffusion que nous avons utilisée dans les sections précédentes a été généralisée dans [59] en introduisant les notions de "plus capable ("*more capable*")" et "moins bruyant ("*less noisy*")" . La relation "le canal 1 est plus capable que le canal 2" est caractérisée par $I(X;Y_1) \geq I(X;Y_2)\ \forall P_X$. La relation "le canal 1 est moins bruyant que le canal 2" est caractérisée par la propriété que pour tout $V \rightarrow X \rightarrow Y_1 Y_2$

$$I(V;Y_1) \geq I(V;Y_2) \tag{2.13}$$

Dans [59], il est montré que la condition “plus capable” est strictement plus faible que la condition “moins bruyant”, qui à son tour, est strictement plus faible que la condition “le canal 2 est une version dégradée du canal 1”. Lorsque le canal 1 est “moins bruyant” que le canal 2, on a $I(V;Y_1) - I(V;Y_2) \leq I(X;Y_1) - I(X;Y_2)$. Ainsi la capacité sécrète dans ce cas est obtenue à partir du corollaire 2 en prenant $V = X$ [9]. On obtient le corollaire suivant :

Corollaire 3 *La capacité secrète du canal à écoute lorsque le canal 1 est “moins bruyant” que le canal 2 est :*

$$R_1 = \max_{P_X} I(X;Y_1) - I(X;Y_2) \tag{2.14}$$

Lorsque le canal 1 est “plus capable” que le canal 2, la capacité secrète est aussi donnée par l'équation (2.14). On note que le canal à écoute a été introduit par Wyner [7] qui a supposé que le canal de l'espion est une version physiquement dégradée du canal du récepteur légitime. La capacité secrète, dans ce cas, est donnée aussi par l'équation (2.14).

La capacité secrète du canal à écoute Gaussien est donnée dans [8] et peut être déduite (lorsque $N_2 > N_1$) du théorème 4 en prenant $\beta = 1$ (la puissance totale est utilisée pour transmettre le message confidentiel) :

$$R_1 = C\left(\frac{P}{N_1}\right) - C\left(\frac{P}{N_2}\right) \tag{2.15}$$

Cette capacité est atteinte en utilisant des entrées Gaussiennes : $X \sim \mathcal{N}(0, P)$.

2.4 Conclusion

Dans ce chapitre, on a fournit les éléments nécessaires à la compréhension du contexte des chapitres suivants. On a présenté les concepts de canal de diffusion et le canal de diffusion avec message confidentiel en donnant des régions des débits atteignables dans les deux cas. Cependant, les schémas qui permettent d'atteindre ces limites théoriques de la communication ne sont pas toujours réalisables en pratique.

En particulier, pour les canaux de diffusion Gaussiens, avec ou sans contrainte de sécurité, on a vu que la région de capacité est atteinte en utilisant des alphabets Gaussiens. Cependant, les alphabets Gaussiens, bien qu'ils maximisent les débits atteignables par les utilisateurs pour les canaux de diffusion Gaussiens, ne sont pas pratiques à implémenter dans les systèmes de communication réels. Dans le chapitre suivant, on étudie l'impact de la contrainte de l'alphabet d'entrée fini sur les régions des débits atteignables pour les canaux de diffusion Gaussiens avec deux utilisateurs. On s'intéresse aussi à étudier le compromis entre l'efficacité des stratégies de diffusion et leur complexité d'implémentation.

De plus, dans les deux modèles de canaux de diffusion étudiés, les régions de débits données sont atteignables lorsque l'émetteur connait l'état instantané du canal (les RSB) ce qui n'est pas toujours le cas dans les systèmes réels. Dans le chapitre 4, on analyse le débit utile secret du canal à écoute à évanouissement par blocs en utilisant les protocoles HARQ lorsque l'émetteur n'a pas une information parfaite sur l'état instantané du canal mais connait seulement les statistiques du canal et reçoit les états passés du canal par l'intermédiaire des canaux de retour.

Chapitre 3

Optimisation des débits atteignables pour les canaux de diffusion avec un alphabet d'entrée fini

Sommaire

3.1 Introduction

On a vu dans le chapitre précédent que le codage par superposition permet d'atteindre la limite théorique de la région de capacité pour un canal de diffusion Gaussien à deux utilisateurs en utilisant un alphabet d'entrée Gaussien pour chaque utilisateur. Cependant, dans les systèmes de transmission réels, les symboles transmis appartiennent à des constellations finies ex. M-PAM et M-QAM.

L'objectif de ce chapitre est de dériver les régions des débits atteignables pour un canal de diffusion Gaussien à deux utilisateurs avec une contrainte de puissance en utilisant des constellations M-PAM dans deux cas : (1) lorsque l'émetteur envoie un message commun pour les deux récepteurs et un message privé pour l'utilisateur 1 (2) le cas du canal de diffusion avec un message confidentiel pour l'utilisateur 1 (et avec un message commun). Les régions des débits atteignables pour les deux cas sont étudiées pour différentes stratégies de transmission qui diffèrent par leur complexité d'implémentation. Un algorithme itératif est proposé pour le calcul des régions des débits atteignables maximales en utilisant le codage par superposition (le cas général) ou le cas particulier du superposition de modulation pour les deux cas des canaux de diffusion considérés. L'optimisation est faite par rapport à la distribution de probabilité jointe ou par rapport aux positions des symboles dans la constellation ou les deux en même temps. Dans notre travail, les positions des symboles ne sont pas nécessairement proportionnelles à celles de la constellation standard comme dans [40]. Cela nous permet de déterminer les débits atteignables maximales avec toute constellation avec M symboles. Évidemment, les meilleurs résultats sont obtenus pour le cas le plus général. L'objectif est d'évaluer la

perte en terme de débits en utilisant les stratégies simples et d'identifier les situations dans lesquelles les schémas complexes (non-standard) conduisent à des améliorations significatives. Comme application, on considère plusieurs scénarios de zones de couverture, et nous donnons des conclusions sur les stratégies de transmission qui peuvent fournir le meilleur compromis entre l'efficacité et la complexité d'implémentation. On compare aussi les deux types de canaux de diffusion considérés (avec et sans contrainte de sécurité) et on analyse l'effet de la contrainte de sécurité sur les débits atteignables.

La plupart des informations de ce chapitre font partie de l'article [1] (voir l'annexe A) et d'un article soumis (voir l'annexe B). Nous résumons ici les résultats principaux. Le chapitre est organisé de la manière suivante :

3.2 Stratégies de transmission pour les systèmes de diffusion

On a vu dans le chapitre précédent que la région de capacité pour le canal de diffusion Gaussien (avec et sans contrainte de sécurité) est atteignable en utilisant le codage par superposition pour transmettre simultanément les deux messages commun et privé/secret. Pour le cas du canal de diffusion avec message confidentiel, un codage stochastique permet d'assurer la sécurité [9],[60].

Dans cette section, on décrit brièvement différentes stratégies de transmission pour les systèmes de diffusion avec deux messages. Les stratégies sont présentées dans l'ordre croissant de complexité de mise en œuvre. Plus précisément, en se déplaçant d'une stratégie à l'autre, on relâche des contraintes sur l'implémentation du système pour atteindre finalement la stratégie la plus complexe qui peut être utilisée pour diffuser des informations vers les utilisateurs. Le passage des stratégies générales aux stratégies les plus simples se fait en ajoutant des contraintes (probabilité uniforme, constellation standard). Ces dernières sont donc les moins efficaces en termes des débits atteignables. Une description détaillée des stratégies est donnée dans [1] (voir l'annexe A). Elles sont listées ci-après.

3.2.1 Partage de temps ou "*Time sharing*" (TS)

Dans le *time sharing*, les messages sont transmis dans des intervalles de temps (*slots*) différents. Le *time sharing* est largement utilisé en raison de sa facilité d'implémentation, puisque dans chaque intervalle de temps le système est équivalent à un système de communication classique point à point. Ici, nous considérons les cas où les symboles transmis sont équiprobables et appartiennent à une constellation M-PAM standard. La constellation M-PAM standard est une constellation avec des symboles équidistants appartenant à $\mathcal{X} = \{M - 1 - 2 \cdot (i-1) \text{ pour } i = 1, .., M\}$.

3.2.2 Modulation hiérarchique (HM)

Dans la modulation hiérarchique avec deux couches, les symboles de la constellation sont utilisés pour transmettre deux flux de données simultanément pour deux utilisateurs [61][62][63]. La modulation hiérarchique a été incluse dans plusieurs standards [23],[24]. Les symboles de la constellation sont généralement choisis avec la même probabilité, mais peuvent être non équidistants. Ces symboles peuvent être considérées comme la somme de deux modulations d'ordre inférieur, une pour chaque utilisateur. La modulation de puissance plus élevée est utilisée pour l'utilisateur ayant le mauvais canal, et celle ayant la puissance la plus petite est utilisée pour l'utilisateur ayant le bon canal. Par conséquent, le codage dans le cas de la modulation hiérarchique peut être séparable pour les deux flux ce qui est plus pratique. Le "*labeling*" de la constellation du signal transmis permet de distinguer les deux types d'information [50],[49]. La modulation hiérarchique est expliquée en [1] avec une constellation 4-PAM comme exemple.

3.2.3 Superposition de modulation (SM)

Pour la superposition de modulation [64], les M points de la constellation appartenant à $\mathcal{X}$ sont obtenus par addition de deux variables aléatoires X_1 et X_2 de cardinalité M_1 et M_2 respectivement : $M = M_1 M_2$. Par exemple, pour un 8-PAM ($M = 8$), on a deux cas de superposition de modulation : soit $M_1 = 2$ et $M_2 = 4$ ou bien $M_1 = 4$

et $M_2 = 2$. Dans ce chapitre, X_1 et X_2 désignent les signaux qui portent l'information pour l'utilisateur 1 (avec ou sans contrainte de sécurité) et l'information commune respectivement. Alors dans ce cas le *labeling* de la constellation est séparable. Cela conduit à $U \equiv X_2$ dans le cas de la superposition de modulation puisque l'utilisateur 2 peut distinguer seulement U. Dans ce cas il y a plus de schémas de labeling que dans le cas de la modulation hiérarchique [50],[49].

Ce travail étudie plusieurs cas de superposition modulation. Nous noterons $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ la superposition de modulation avec symboles équiprobables. Il s'agit d'un cas pratique puisque le codage des messages est séparable et les symboles sont utilisés avec la même probabilité ce qui est le cas dans les systèmes actuels. Ensuite, la contrainte "symboles équiprobables" est relâchée et on suppose que P_{UX} peut être non-uniforme. Ainsi, le codage est ici fait conjointement pour les deux messages. Cette stratégie sera notée $SM_{\overline{\mathcal{X}},P_{UX},P_X}$ quand les symboles prennent les valeurs de la constellation standard et $SM_{\mathcal{X},P_{UX},P_X}$ dans le cas où les positions des symboles peuvent prendre des valeurs arbitraires et seront considérés comme des variables à optimiser. De manière générale, une variable est surlignée lorsqu'elle n'intervient pas dans le processus d'optimisation.

La définition de la superposition de modulation dans le cas général où P_{UX} peut être non-uniforme est donnée dans [1]. La distribution de probabilité jointe P_{UX} a alors une expression spécifique ce qui est expliquée dans [1] pour le cas d'une 8-PAM.

3.2.4 Codage par superposition (SC)

Dans le codage par superposition, la distribution de probabilité jointe P_{UX} prend la forme la plus générale, *i.e.* lorsque $|\mathcal{U}| = |\mathcal{X}|$ pour les canaux de diffusion Gaussiens. Dans le cas d'une constellation avec M symboles, P_{UX} est une matrice de taille $M \times M$ avec des éléments p_{ij}. En effet, la variable auxiliaire U peut être vue comme le "centre du nuage" d'information contrairement aux cas les plus simples où le message commun est porté par le centre des nuages de la ***modulation***. Par conséquence, le *labeling* ne permet pas de distinguer les information portées par les deux messages. Cela rend ce schéma de codage plus compliqué. Le codage des deux messages est fait conjointement

Transmission	Variables	Contraintes	Désignation
SM	$\mathcal{X}$	Distribution uniforme pour P_{UX}	$SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$
SM	P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$	Positions des symboles : M-PAM	$SM_{\overline{\mathcal{X}},P_{UX},P_X}$
SM	$\mathcal{X}$ P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$		$SM_{\mathcal{X},P_{UX},P_X}$
SC	P_{UX} s.t. $\sum_i p_{i,j} = \frac{1}{M}$	Positions des symboles : M-PAM Distribution uniforme pour P_X	$SC_{\overline{\mathcal{X}},P_{UX},\overline{P_X}}$
SC	$\mathcal{X}$ P_{UX} s.t. $\sum_i p_{i,j} = \frac{1}{M}$	Distribution uniforme pour P_X	$SC_{\mathcal{X},P_{UX},\overline{P_X}}$
SC	P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$	Positions des symboles : M-PAM	$SC_{\overline{\mathcal{X}},P_{UX},P_X}$
SC	$\mathcal{X}$ P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$		$SC_{\mathcal{X},P_{UX},P_X}$

TABLE 3.1 – Stratégies de diffusion considérées

en utilisant la distribution de probabilité jointe P_{UX} comme indiqué dans le chapitre 2.

Une liste exhaustive de toutes les stratégies considérées est donnée dans le tableau 3.1.

3.3 Régions des débits atteignables en utilisant des constellations M-PAM : formulation du problème

Dans ce paragraphe, on s'intéresse au calcul des régions des débits atteignables pour un canal de diffusion Gaussien avec deux utilisateurs et une contrainte de puissance lorsque le signal transmis est modulé en utilisant une constellation M-PAM pour les différentes stratégies de diffusion décrites ci-dessus.

Comme indiqué au début de ce chapitre, on va étudier deux modèles du canal de diffusion lorsqu'il y a en plus d'un message commun w_0 pour les deux récepteurs, (i) un

message privé w_1 pour le récepteur 1, mais pas nécessairement secret, dans le premier cas (voir le paragraphe 2.2) (ii) un message secret w_1 pour le récepteur 1 dans le deuxième cas (voir le paragraphe 2.3).

Considérons un canal de diffusion Gaussien sans-mémoire avec deux utilisateurs ($RSB_1 > RSB_2$) et une contrainte de puissance P. L'entrée du canal appartient à un ensemble fini $\mathcal{X} = \{x_0, ..., x_{M-1}\} \subset \mathbb{R}$ représenté par une constellation M-PAM. On suppose que la constellation du signal transmis est symétrique par rapport à l'origine.

Pour déterminer la région des débits atteignables maximales en utilisant le codage par superposition, on considère le cas $|\mathcal{U}| = M$. Dans le cas de la superposition de modulation, il faut prendre en compte les spécificités sur P_{UX} et $\mathcal{X}$ [1]. On considère également dans le même contexte, le problème de maximisation des débits atteignables sous des contraintes supplémentaires sur les variables d'optimisation (P_{UX} et $\mathcal{X}$) : valeurs standards des positions des symboles du M-PAM, distribution P_{UX} uniforme, distribution P_X uniforme. Le problème de maximisation des débits atteignables pour une certaine stratégie est résolu sous différentes combinaisons des contraintes précédentes selon le tableau 3.1.

3.3.1 Cas du canal de diffusion avec message commun et message privé

On rappelle que dans ce modèle, le message w_0 est un message commun aux deux récepteurs et w_1 est un message privé à l'utilisateur 1. Par conséquent, le récepteur 1 atteint un débit R_0+R_1 tandis que le récepteur 2 atteint un débit R_0. Ainsi, la région des débits atteignables (R_0 vs R_0+R_1) peut être obtenue en résolvant la maximisation de la somme des débits pondérée ($\theta \cdot R_1 + (1-\theta) \cdot R_0$) pour $\theta \in [0, 0.5]$. En effet, pour $\theta = 0$, on maximise le débit de l'information commune R_0 et lorsque $\theta = 0.5$, on maximise le débit atteint par l'utilisateur 1 ($R_0 + R_1$). En utilisant (2.1) et (2.2), le problème d'optimisation considéré est :

$$\begin{aligned} \max_{P_{UX},\mathcal{X}} \quad & \theta \cdot I(X;Y_1|U) + (1-\theta) \cdot I(U;Y_2) \\ s.t. \quad & \begin{cases} p_{ij} \geq 0 \quad \forall i,j \\ \sum_{i,j} p_{ij} \cdot x_j^2 \leq P \end{cases} \end{aligned} \tag{3.1}$$

Cette optimisation est faite en considérant les contraintes données dans le tableau 3.1 pour chaque stratégie de transmission considérée. Notons $p_{ij} = \Pr\{U = u_i, X = x_i\}$, $j \in \{0,..,M-1\}$ et $i \in \{0,..,|\mathcal{U}|-1\}$. Les expressions des deux information mutuelles $I(X;Y_k|U)$ et $I(U;Y_2)$ sont les suivantes, pour $k \in \{1,2\}$:

$$I(X;Y_k|U) = \sum_{i,j} \int_{-\infty}^{+\infty} p_{ij} P_{Y_k|X}(y_k|x_j) \log \frac{(\sum_{j'} p_{ij'}) P_{Y_k|X}(y_k|x_j)}{\sum_{j'} p_{ij'} P_{Y_k|X}(y_k|x_{j'})} dy_k \tag{3.2}$$

$$I(U;Y_2) = \sum_{i} \int_{-\infty}^{+\infty} (\sum_{j} p_{ij} P_{Y_2|X}(y_2|x_j)) \log \frac{\sum_{j'} p_{ij'} P_{Y_2|X}(y_2|x_{j'})}{(\sum_{j'} p_{ij'})(\sum_{i',j'} p_{i'j'} P_{Y_2|X}(y_2|x_{j'}))} dy_2 \tag{3.3}$$

Les logarithmes sont pris en base 2. Le canal Gaussien pour chaque utilisateur est caractérisé par la densité conditionnelle

$$P_{Y_i|X}(y|x) = \frac{1}{\sqrt{2\pi\sigma_i^2}} . e^{-\frac{(y-x)^2}{2\sigma_i^2}} \quad i \in \{1,2\} \tag{3.4}$$

Quand $\theta = 0$ ou $\theta = 1$ (le cas du canal point-à-point (PàP)), on maximise respectivement les débits atteignables individuels R_0 et R_1. Le problème (3.1) est équivalent à

$$\begin{aligned} \max_{P_X,\mathcal{X}} \quad & I(X;Y_k) \\ s.t. \quad & \begin{cases} p_i \geq 0 \quad \forall i \\ \sum_i p_i = 1 \\ \sum_i p_i \cdot x_i^2 \leq P \end{cases} \end{aligned} \tag{3.5}$$

où $p_i = \Pr\{X = x_i\}$, $i \in \{0,..,M-1\}$ est la distribution de probabilité des symboles d'entrée du canal et $k \in \{1,2\}$. Lorsque $\theta = 0$ ou 1, le problème (3.5) est résolu pour $k = 2$ et 1 respectivement avec :

$$I(X;Y_k) = \int_{-\infty}^{+\infty} \sum_{j} p_j P_{Y_k|X}(y_k|x_j) \log \frac{P_{Y_k|X}(y_k|x_j)}{\sum_{j'} p_{j'} P_{Y_k|X}(y_k|x_{j'})} dy_k \tag{3.6}$$

Pour le cas du *time sharing* et en utilisant une constellation standard, la paire de débits atteignables $(R_0 + R_1, R_0)$ est telle que [5] :

$$\begin{cases} R_1 = \alpha\overline{R_1} \\ R_0 = (1-\alpha)\overline{R_0} \end{cases} \tag{3.7}$$

où $\overline{R_1}$ et $\overline{R_0}$ sont les débits atteignables pour un canal point-à-point en utilisant une constellation M-PAM standard avec des rapports signal sur bruit RSB_1 et RSB_2 respectivement. En variant α de 0 à 1, on obtient la région des débits atteignables.

3.3.2 Cas du canal de diffusion avec message commun et message confidentiel

Dans ce paragraphe, on étudie le cas où l'émetteur veut transmettre un message secret w_1 pour l'utilisateur 1 en présence de l'espion (l'utilisateur 2) avec un débit R_1 et un message commun w_0 pour les deux utilisateurs avec un débit R_0. Alors, les utilisateurs 1 et 2 peuvent atteindre un débit $R_0 + R_1$ et R_0 respectivement. Cependant, dans ce cas, on a préféré étudier les régions R_0 vs R_1 (et non pas $R_0 + R_1$ vs R_0 comme dans le cas précédant), obtenues en résolvant la somme de débits pondérée $\theta \cdot R_1 + (1-\theta) \cdot R_0$ pour $\theta \in [0, 1]$. Ce choix permet de mieux étudier l'effet de la contrainte de sécurité qui distingue ce cas du cas précédent. On notera qu'il est impossible d'avoir un débit secret positif si RSB_2 n'est pas inférieure à RSB_1 .

Pour déterminer la région des débits atteignables en utilisant une certaine stratégie de diffusion, il faut résoudre le problème d'optimisation suivant issu des équations (2.9) et (2.10) :

$$\begin{aligned} &\max_{P_{UX}, \mathcal{X}} \quad \theta \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U) \Big] + (1-\theta) \cdot I(U;Y_2) \\ &s.t. \quad \begin{cases} p_{ij} \geq 0 \quad \forall (i,j) \\ \sum_{ij} p_{ij} \cdot x_j^2 \leq P \\ \sum_{ij} p_{ij} = 1 \end{cases} \end{aligned} \tag{3.8}$$

avec $\theta \in [0,1]$, $p_{ij} = \Pr\{U = u_i, X = x_j\}$, $j \in \{0, .., M-1\}$ et $i \in \{0, .., |\mathcal{U}| - 1\}$. Lorsque P_X est contrainte à être uniforme, la dernière équation doit être remplacée par

$\sum_i p_{ij} = \frac{1}{M}$. Pour le cas du *time sharing*, les débits atteignables sont obtenus par la même méthode que le paragraphe 3.3.1.

Quand $\theta = 1$, le problème (3.8) est équivalent à la maximisation du débit secret atteignable $R_1 = I(X;Y_1) - I(X;Y_2)$ sous une contrainte de puissance pour un canal à écoute Gaussien par rapport à P_X et $\mathcal{X}$ [9].

Les problèmes (3.1) et (3.8) sont des problèmes d'optimisation non-convexes. La méthode de recherche exhaustive n'est pas envisageable pour résoudre des problèmes ayant un nombre aussi important de variables. Pour résoudre (3.1) et (3.8), une méthode itérative est proposée dans le paragraphe suivant.

3.4 Algorithme d'optimisation

Dans ce paragraphe, on présente un algorithme d'optimisation qui utilise fondamentalement les mêmes outils pour résoudre les deux problèmes (3.1) et (3.8). Certaines adaptations ou variantes sont parfois nécessaires. Nous les discuterons ensuite pour chacune des situations.

Nous considérons tout d'abord une version régularisée de (3.1) :

$$L_1(\mathcal{X}, P_{UX}, s) = \theta \cdot I(X;Y_1|U) + (1-\theta) \cdot I(U;Y_2) + s \cdot (P - \sum_{i=0}^{|\mathcal{U}|-1} \sum_{j=0}^{M-1} p_{ij} \cdot x_j^2) \quad (3.9)$$

et une version régularisée du problème (3.8) :

$$L_2(\mathcal{X}, P_{UX}, s) = \theta \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U)\Big] + (1-\theta) \cdot I(U;Y_2) + s \cdot \Big(P - \sum_{ij} p_{ij} \cdot x_j^2\Big) \quad (3.10)$$

où s est un paramètre de régularisation.

Pour une valeur donnée de s, les problèmes d'optimisation (3.9) et (3.10) sont résolus (pour le cas le plus général) par rapport à P_{UX} et $\mathcal{X} = (x_0, x_1, ..., x_{M-1})$ alternativement jusqu'à convergence :

$$P_{UX}^{(\ell)} = \arg \max_{P_{UX} \in \mathcal{C}} L(P_{UX}, x_0^{(\ell-1)}, .., x_{M-1}^{(\ell-1)}, s) \quad (3.11)$$

$$\mathcal{X}^{(\ell)} = \arg\max_{\mathcal{X}} L(P_{UX}^{(\ell)}, x_0, .., x_{M-1}, s) \tag{3.12}$$

où $L = L_1$ lorsqu'on veut résoudre le problème (3.1) et $L = L_2$ lorsqu'on veut résoudre le problème (3.8), ℓ est l'indice d'itération et $\mathcal{C}$ désigne l'ensemble des contraintes sur P_{UX}. On définira $\mathcal{C}$ soit comme $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$ ou $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_i p_{i,j} = \frac{1}{M}\}$ (symboles équiprobables).

On commence à expliquer la méthode pour résoudre le problème d'optimisation dans (3.12). La fonction $L(P_{UX}^{(\ell)}, x_0, .., x_{M-1}, s)$ n'est pas une fonction concave pour tout $\mathcal{X} \in \mathbb{R}^M$. Cependant, nous avons observé dans nos expériences que $L(P_{UX}^{(\ell)}, x_0, .., x_{M-1}, s)$ est une fonction concave si $\mathcal{X} \in \mathcal{D}$ où $\mathcal{D} = \{\mathcal{X} \in \mathbb{R}^M : |x_i - x_j| > d \quad \forall i, j \in \{0, .., M-1\}$ and $i \neq j\}$ et d dépend de la taille de la constellation et du RSB. Une méthode du simplexe est ensuite utilisée pour effectuer l'optimisation avec une initialisation faite dans $\mathcal{D}$. Cette méthode s'applique pour les deux cas : $L = L_1$ et $L = L_2$. La figure 3.1, montre un exemple du contour du lagrangien L en fonction des positions des symboles x_0 et x_1 d'une constellation 4-PAM ($\mathcal{X} = \{x_0, x_1, -x_1, -x_0\}$) pour chacun des cas $L = L_1$ et $L = L_2$ et avec P_{UX} fixé. On a observé dans les deux cas, que le Lagrangien possède un optimum global situé dans la région telle que $x_0 > x_1$ et un optimum local situé dans la région $x_0 < x_1$. Par suite, dans le cas du 4-PAM, on a fait deux initialisations de x_0 et x_1 pour appliquer la méthode du simplexe. Il est clair aussi que la région telle que x_0 et x_1 sont très proches est à éviter dans les initialisations, car la fonction à optimiser possède des minimums dans cette région.

Considérons maintenant le problème (3.11) lorsque P_{UX} n'est pas contrainte à être uniforme. Dans la littérature, il existe dans [65] un algorithme de type Blahut-Arimoto modifié [66] pour résoudre le problème d'optimisation dans (3.11) pour $L = L_1$ avec l'ensemble de contraintes $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$. Cependant, cet algorithme ne tient pas compte de la contrainte de puissance. Pour le cas du canal de diffusion avec message confidentiel, il existe aussi un algorithme de type Blahut-Arimoto qui permet de maximiser le débit secret $I(X;Y_1) - I(X;Y_2)$ (lorsque $U = const.$) pour le canal à écoute lorsque le canal du légitime est moins bruyant que celui de l'espion. Cet algorithme proposé dans [67] est garanti à converger vers le maximum global puisque la fonction

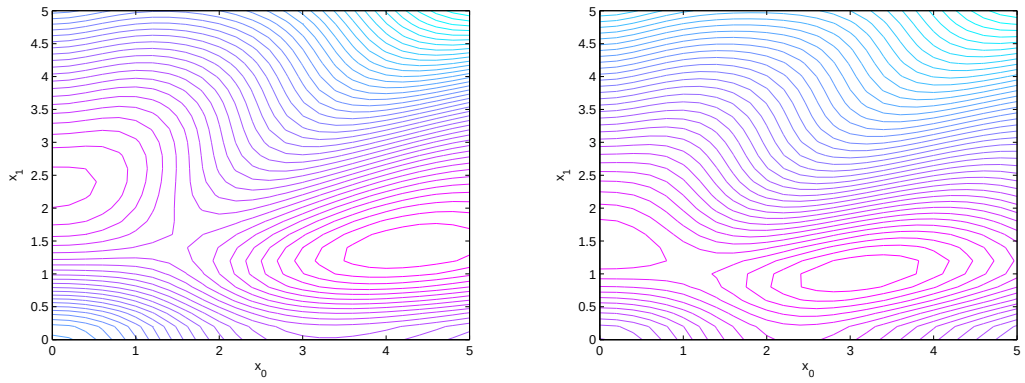

FIGURE 3.1 – Contour du Lagrangien L où RSB_1=10 dB, RSB_2=4 dB, s=0.03, P_{UX} arbitraire. **A gauche :** pour $L = L_1$, θ=0.45, le maximum correspond à ($x_0 = 4.4$, $x_1 = 1.4$). **A droite :** pour $L = L_2$, θ=0.7, le maximum correspond à ($x_0 = 3$, $x_1 = 1$).

$I(X;Y_1) - I(X;Y_2)$ est concave en P_X pour $\mathcal{X}$ fixée dans ce cas [68]. Dans [69], il est montré que l'algorithme proposé dans [67] est aussi utile dans le cas où le canal du légitime est plus capable que celui de l'espion (si le point initial est bien choisi).

Introduisons maintenant le lemme suivant :

Lemme 1

(i) $I(X;Y_1|U)$ *est concave en* P_{UX}*,*

(ii) $I(U;Y_2)$ *est une différence de fonctions concaves en* P_{UX}*,*

(iii) $I(X;Y_1|U) - I(X;Y_2|U)$ *est concave en* P_{UX} *si et seulement si le canal du récepteur légitime est moins bruyant que le canal de l'espion.* □

où (i) et (ii) sont démontrés dans [70] et (iii) est démontré dans [54] (voir Annexe B). Alors, le problème (3.11) est un problème d'optimisation non-convexe.

A partir des expressions des informations mutuelles $I(X;Y_1|U)$, $I(X;Y_2|U)$ et $I(U;Y_2)$, on a le lemme suivant :

Lemme 2 *Considérons le cas du codage par superposition où le signal transmis* X *n'est pas une somme des signaux* X_2 *et* X_1 *portant l'information commune et l'information pour l'utilisateur 1 (avec ou sans contrainte de sécurité) respectivement. Dans ce cas,*

si $P_{UX}^{*(l)}(s)$ *est une solution du problème (3.11), alors toute distribution* P_{UX} *obtenue en permutant les lignes de* $P_{UX}^{*(l)}(s)$ *est aussi une solution du problème (3.11).* □

Le lemme 2 vient des équations (3.2), (3.3) et les contraintes dans les problèmes (3.1) et (3.8) où la permutation des lignes de la distribution de probabilité jointe ne change pas la valeur de la fonction dans (3.11). Par conséquent, le problème (3.11) a des solutions multiples. Cependant le lemme 2 ne s'applique pas pour le cas de la superposition de modulation, puisque $\mathcal{U}$ représente l'alphabet de l'information commune ($U = X_2$). Par suite, les positions des symboles de la constellation $\mathcal{X}$ dépendent des valeurs de $\mathcal{U}$, *i.e.* $X = U + X_1$ où X_1 représente le signal pour le récepteur 1. Par conséquent, la permutation des lignes de P_{UX} va changer les valeurs des information mutuelles dans (3.2), (3.3) pour la stratégie du superposition de modulation.

Par conséquent, il est évident que dans certaines situations considérées, le problème d'optimisation (3.11) a plusieurs solutions et le maximum global n'est pas unique. Cela est précisé ci-dessous.

Lorsque $\mathbf{L} = \mathbf{L_1}$, le problème d'optimisation dans (3.11) avec l'ensemble de contraintes $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$ peut être manipulé par un algorithme de type Blahut-Arimoto proposé dans [65]. En effet, afin de tenir compte de la régularisation, on peut montrer que l'algorithme de type "Blahut Arimoto "proposé dans [65] pour les canaux de diffusion dégradés devrait être modifié en remplaçant l'équation (19) du "lemma 3" dans [65] par $q^*(u,x) = \frac{\beta[Q,\tilde{Q},\bar{Q}](u,x)\cdot e^{-s\frac{x^2}{1-\theta}}}{\sum_{u',x'}\beta[Q,\tilde{Q},\bar{Q}](u',x')\cdot e^{-s\frac{x'^2}{1-\theta}}}$ au lieu de $q^*(u,x) = \frac{\beta[Q,\tilde{Q},\bar{Q}](u,x)}{\sum_{u',x'}\beta[Q,\tilde{Q},\bar{Q}](u',x')}$ où $\beta[Q,\tilde{Q},\bar{Q}](u,x)$ est défini dans l'équation (19) du référence [65]. Quand il y a une contrainte supplémentaire sur les symboles de la constellation d'être équiprobables *i.e.* $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1 \quad \text{and} \quad \sum_i p_{i,j} = \frac{1}{M}\}$, l'algorithme de type "Blahut Arimoto "dans [65] devrait également être modifié pour tenir compte de la contrainte supplémentaire. Dans ce cas , l'équation (19) du "lemma 3" dans la référence [65] devrait être remplacé par $q^*(u,x) = \frac{1}{|\mathcal{X}|}\cdot\frac{\beta[Q,\tilde{Q},\bar{Q}](u,x)}{\sum_u \beta[Q,\tilde{Q},\bar{Q}](u,x)}$, qui ne dépend pas de s, où $\beta[Q,\tilde{Q},\bar{Q}](u,x)$ est défini dans l'équation (19) dans cette référence.

Lorsque $\mathbf{L} = \mathbf{L_2}$, et pour résoudre le problème d'optimisation dans (3.11), on a

utilisé un algorithme de type Blahut-Arimoto qui peut être fait pour le cas du canal de diffusion avec message confidentiel en utilisant la même méthode de l'algorithme proposé pour le canal de diffusion dégradé sans contrainte de sécurité [65][1]. Cet algorithme utilisé pour le cas du canal de diffusion avec message confidentiel est une généralisation de celui proposé dans [67] (l'algorithme proposé dans [67] est un cas particulier de l'algorithme de type Blahut-Arimoto pour le canal de diffusion avec message confidentiel lorsque $\theta = 1$).

Cependant, puisque (3.11) n'est pas convexe en P_{UX}, l'algorithme de type Blahut-Arimoto converge dans [65] lorsque certaines conditions sont satisfaites. Ces conditions sont données dans le théorème 2 du [65]. En effet, si la solution de (3.11), $P_{UX}^{*(l)}(s)$, se situe dans un ensemble $T_{k,\theta}(\tilde{P}_{UX})$ et que la fonction $L(P_{UX}, \mathcal{X}^{(\ell-1)}, s)$ est concave en $T_{k,\theta}(\tilde{P}_{UX})$ et que la valeur initiale $P_{UX}^{(0)(l)}(s) \in T_{k,\theta}(\tilde{P}_{UX})$, l'algorithme de type Blahut-Arimoto converge vers la valeur optimale. $T_{k,\theta}(\tilde{P}_{UX})$ est aussi défini dans [65] comme l'ensemble de tous les points $P_{UX} \in S_{k,\theta} \triangleq \{P_{UX} | L(P_{UX}, \mathcal{X}^{(\ell-1)}, s) \geq k\}$ tel que P_{UX} est accessible à partir de $\tilde{P}_{UX} \in S_{k,\theta}$ par un chemin continu. Par suite, le problème est maintenant de choisir un point initial approprié.

Dans les expériences, on constate que la région $T_{k,\theta}(\tilde{P}_{UX})$ où la fonction objective dans (3.11) est concave en P_{UX} est plus grande quand θ augmente. Cela est dû au fait que le poids donné à la partie concave de la fonction (*i.e.* $I(X;Y_1|U)$ si $L = L_1$ ou $I(X;Y_1|U) - I(X;Y_2|U)$ si $L = L_2$) augmente avec θ. Par suite il y a plus de chance que l'algorithme converge à partir du point initial dans ce cas. Dans nos expériences, les valeurs initiales sont choisies d'une manière aléatoire et l'algorithme de type Blahut-Arimoto converge vers des solutions raisonnables. Les initialisations à éviter sont la distribution uniforme de P_{UX} parce que dans ce cas, on a observé que l'algorithme converge vers la même distribution , et aussi quand il y a des similitudes dans matrice initiale P_{UX} : *ex.* lorsque deux lignes de la matrice initiale P_{UX} sont identiques l'algorithme de type Blahut Arimoto converge vers un point où P_{UX} possède deux lignes identiques. Dans le cas général du codage par superposition, l'algorithme converge vers une des $M!$ solutions (lemma 2). Notons que lorsque $\theta = 0$, les maximums de $I(U;Y_2)$ sont obtenus

quand $U \equiv X$. Puisque la région $T_{k,\theta}(\tilde{P}_{UX})$ où la fonction objective dans (3.11) est concave en P_{UX} est petite pour les valeurs de θ proches de 0, le point initial doit être proche à la solution optimale pour $\theta = 0$ dans ces cas.

La méthode de maximisation alternative peut au moins augmenter la valeur de la fonction objective dans chaque itération. Dans les expériences, nous avons constaté que cette méthode converge au moins vers un maximum local (désigné par $p^*_{i,j}(s)$, $x^*_j(s)$, $0 \leq j \leq M-1$, $0 \leq i \leq |\mathcal{U}|-1$).

On discute maintenant le choix de s. Comme on ne sait pas quelle valeur a priori de s peut correspondre à la satisfaction de la contrainte de puissance, on propose d'utiliser un processus itératif comme suit :

$$s^{(k+1)} = \left[s^{(k)} - \gamma \cdot \left(P - \sum_{i=0}^{|\mathcal{U}|-1} \sum_{j=0}^{M-1} p^*_{ij}(s^{(k)}) \cdot (x^*_j(s^{(k)}))^2 \right) \right]^+ \tag{3.13}$$

où $[.]^+$ est défini comme $[.]^+ = \max(., 0)$. La valeur de s est augmentée ou diminuée avec le signe de $P - \sum_{i=0}^{|\mathcal{U}|-1} \sum_{j=0}^{M-1} p^*_{ij}(s^{(k)}) \cdot (x^*_j(s^{(k)}))^2$. L'algorithme proposé est résumé dans le tableau 4.1. Évidemment, lorsque les symboles de la constellation prennent les valeurs d'une constellation standard, (P2) qui est définie dans le tableau 4.1 ne sera pas utilisée. De même, lorsque P_{UX} est uniforme, (P1) n'est pas utilisée.

3.5 Analyse des résultats

3.5.1 Canal point-à-point

On présente dans cette section, les résultats de la maximisation des débits atteignables pour le cas du canal point-à-point (PàP) en utilisant des constellations M-PAM avec M=4, 8, 16 et pour différentes valeurs du *RSB*. Pour évaluer la contribution de la mise en forme de constellation, on compare, pour un *RSB* fixe, le débit maximal atteignable et le débit atteignable en utilisant une "constellation standard", dont les symboles sont équiprobables, en termes de gain sur le *RSB* (appelé " *shaping gain*"). Le "*shaping gain*" représenté dans la Fig. (3.2) est le gain obtenu avec une constellation entièrement optimisée ($P_{\mathcal{X}}$ et $\mathcal{X}$) par rapport à la constellation standard M-PAM

Étape 0	$s \leftarrow s^{(0)}$	
Étape k	Étape 0	$\mathcal{X} \leftarrow \mathcal{X}^{(0)}$ où $\mathcal{X} = (x_0, x_1, .., x_{M-1})$
	Étape ℓ	$P_{UX}^{(\ell)} = \arg\max_{P_{UX} \in \mathcal{C}} L(P_{UX}, \mathcal{X}^{(\ell-1)}, s^{(k-1)})$ $(P1)$ $\mathcal{X}^{(\ell)} = \arg\max_{\mathcal{X}} L(P_{UX}^{(\ell)}, \mathcal{X}, s^{(k-1)})$ $(P2)$
	Critère d'arrêt	$\lvert L(P_{UX}^{(\ell)}, \mathcal{X}^{(\ell)}, s^{(k)}) - L(P_{UX}^{(\ell-1)}, \mathcal{X}^{(\ell-1)}, s^{(k-1)}) \rvert \leq \epsilon_L$
	$s^{(k)} = [s^{(k-1)} - \beta(P - \sum_{i,j} p_{ij}^*(s^{(k-1)}) \cdot (x_j^*(s^{(k-1)}))^2)]^+$ où $[.]^+ = \max(., 0)$	
Critère d'arrêt	$\lvert s^{(k)} - s^{(k-1)} \rvert \leq \epsilon_s$	

TABLE 3.2 – Solution numérique pour résoudre (3.1) et (3.8)

dont les symboles sont équiprobables. Afin d'éviter la complexité de la construction de codes approchant du débit maximal, une autre méthode pour faire la mise en forme de constellation est d'optimiser seulement la position des symboles dans la constellation. Chaque point de la constellation est supposé être choisi avec la même probabilité cependant la position de chaque point de la constellation est optimisé. Le *shaping gain* correspondant est donné dans Fig. (3.3). On fait les observations suivantes. Le *shaping gain* dépend du *RSB* et de la taille de la constellation. Le gain maximal est obtenu pour les *RSB* moyens. La distribution de probabilité $P_{\mathcal{X}}$ est très similaire à celle que l'on obtiendrait par l'échantillonnage d'une distribution gaussienne. Avec une constellation à moitié-optimisée ($\mathcal{X}$ seulement), une dégradation significative est observée pour les *RSB* moyens par rapport à la constellation entièrement optimisée. Par conséquent, on peut conclure que l'optimisation de la densité de probabilité des symboles est inutile pour les petites et les grandes valeurs du *RSB* alors que la constellation entièrement optimisée est efficace pour les *RSB* moyens, où le gain augmente avec le la taille de la constellation.

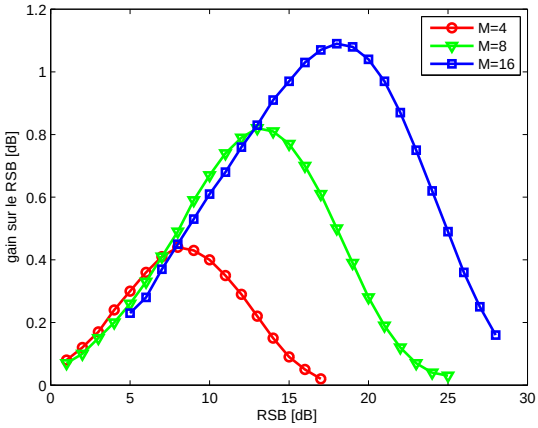

FIGURE 3.2 – Le gain sur le *RSB* pour la constellation entièrement optimisée par rapport à la constellation standard en fonction du *RSB* pour le canal PàP

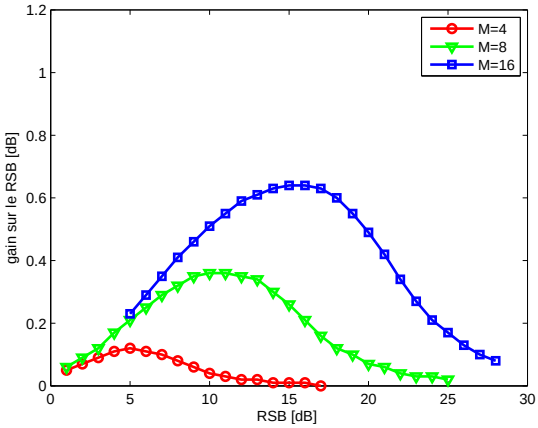

FIGURE 3.3 – Le gain sur le *RSB* pour la constellation à moitié-optimisée ($\mathcal{X}$ seulement) par rapport à la constellation standard en fonction du *RSB* pour le canal PàP

3.5.2 Canal de diffusion

Dans cette section, on présente les principaux résultats sur le calcul des régions de débits atteignables pour le canal de diffusion Gaussien avec deux utilisateurs, sans et avec contrainte de sécurité, en utilisant différentes stratégies de transmission. l'effet de la mise en forme de la constellation est évalué en analysant les courbes des régions de débits atteignables obtenues avec une constellation M-PAM ($M = 4, 8, 16$) pour plusieurs paires (RSB_1, RSB_2). Les stratégies évoquées dans le tableau 3.1 et aussi le *time sharing* seront considérées. Les comparaisons entre les différentes stratégies sont faites en termes de gain sur le RSB pour des débits atteignables cibles (*shaping gain*) et aussi en terme de pourcentage de gain en débit (voir Définitions 1 et 2 dans [1]).

Superposition de modulation

Les courbes des régions des débits atteignables (Fig. 3.4-3.11) pour les deux cas des canaux de diffusion considérés, montrent qu'une amélioration en débits peut être obtenue, selon l'écart entre les RSB des utilisateurs, en optimisant à la fois les positions des symboles dans la constellation et la distribution de probabilité jointe P_{UX} ($SM_{\mathcal{X},P_{UX},P_X}$) par rapport au cas où on optimise seulement les positions des symboles ($SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$). L'analyse du gain maximal en débit atteignable et du gain sur le RSB montre qu'un petit gain en terme de débits atteignables peut se traduire en un gain important en terme du RSB. Les gains maximaux sur le RSB sont donnés dans les annexes A et B. Les gains maximaux sur le RSB augmentent avec la taille M de la constellation. La mise en forme de constellation semble donc plus utile pour les grandes valeurs de M. On constate aussi que le gain maximal sur le RSB devient petit quand l'écart entre le RSB des utilisateurs augmente, indépendamment de M. L'analyse de la matrice optimale P_{UX} aboutit à la conclusion que X_1 et X_2 ne sont pas indépendant en général en utilisant des constellations de taille finie. Finalement, le cas où on optimise seulement P_{UX} alors que les symboles prennent les valeurs de la constellation standard ne semble pas avoir d'intérêt dans les cas étudiés [1], puisque en général, cette stratégie ne s'avère pas efficace en terme de débits atteignables par rapport à $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ alors qu'elle est

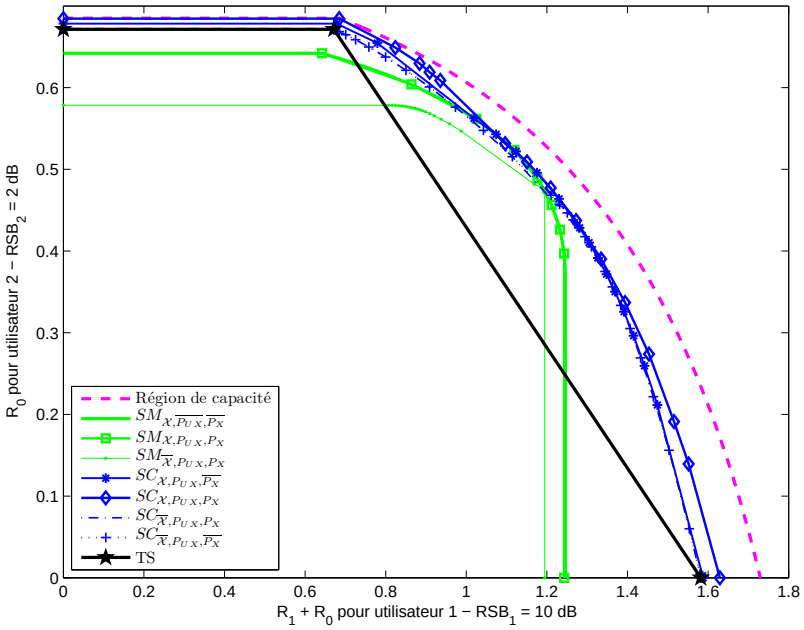

FIGURE 3.4 – Régions des débits atteignables avec $M = 4$ et $(RSB_1, RSB_2) = (10dB, 2dB)$

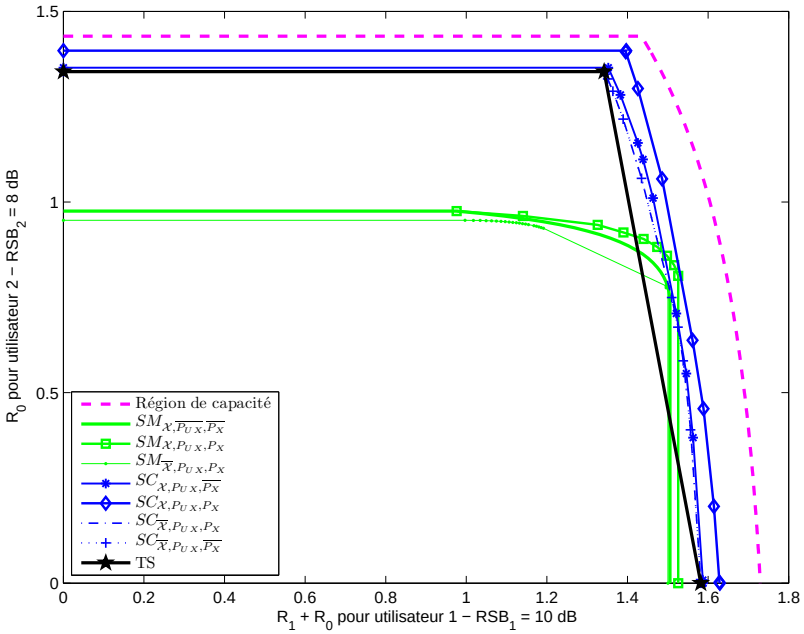

FIGURE 3.5 – Régions des débits atteignables avec $M = 4$ et $(RSB_1, RSB_2) = (10dB, 8dB)$

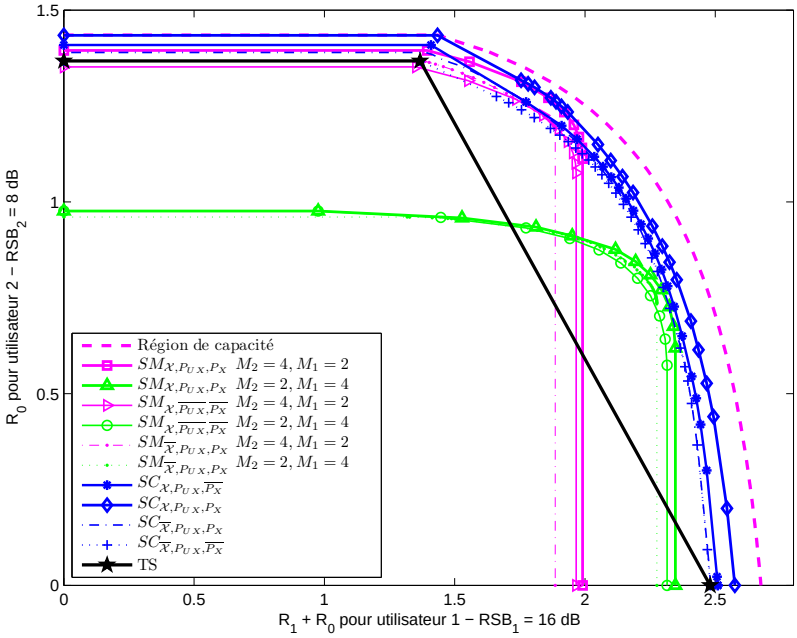

FIGURE 3.6 – Régions des débits atteignables avec $M = 8$ et $(RSB_1, RSB_2) = (16dB, 8dB)$

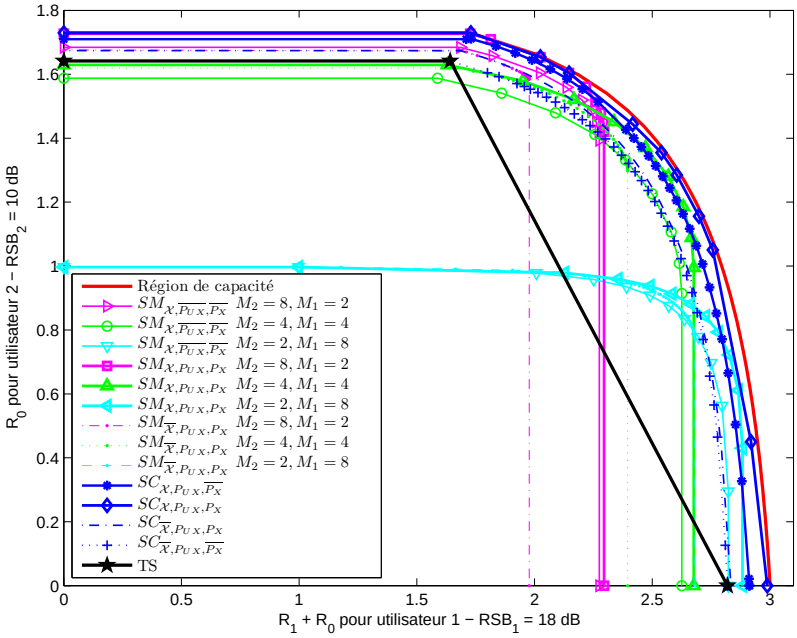

FIGURE 3.7 – Régions des débits atteignables avec $M = 16$ et $(RSB_1, RSB_2) = (18dB, 10dB)$

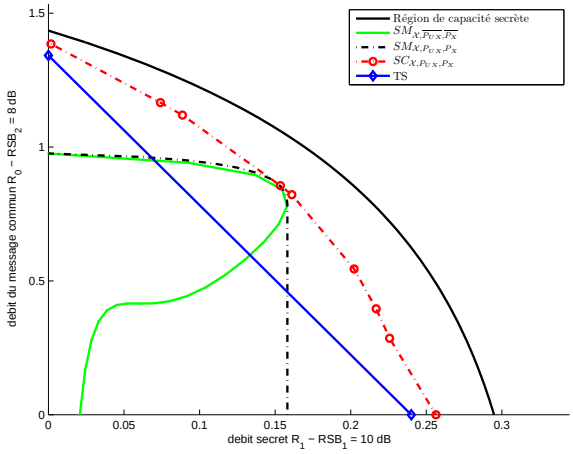

FIGURE 3.8 – Régions des débits atteignables avec contrainte de sécurité. $M = 4$ et $(RSB_1, RSB_2) = (10, 8)$ dB

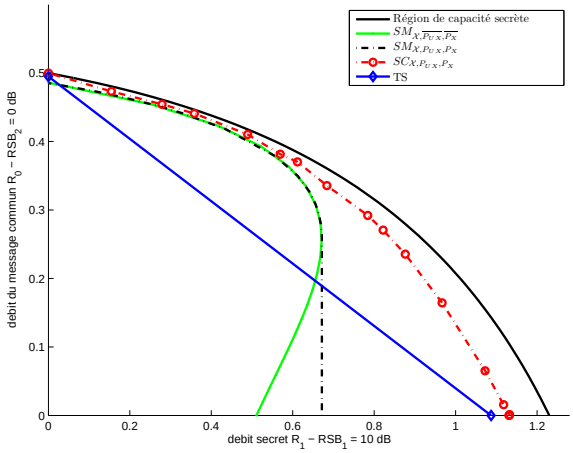

FIGURE 3.9 – Régions des débits atteignables avec contrainte de sécurité. $M = 4$ et $(RSB_1, RSB_2) = (10, 0)$ dB

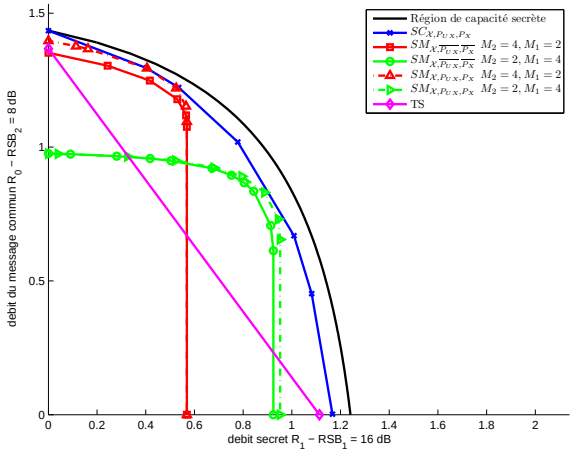

FIGURE 3.10 – Régions des débits atteignables avec contrainte de sécurité. $M = 8$ et $(RSB_1, RSB_2) = (16, 8)$ dB

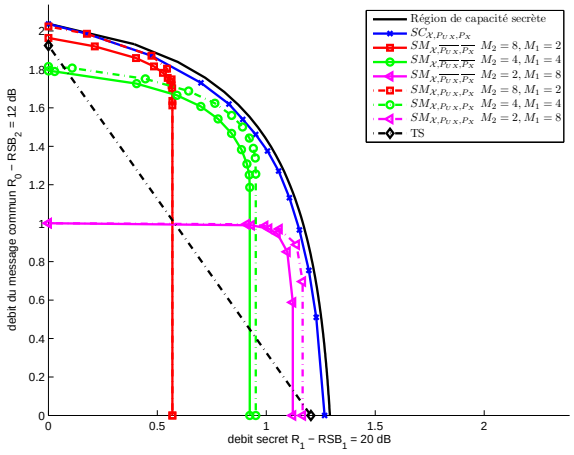

FIGURE 3.11 – Régions des débits atteignables avec contrainte de sécurité. $M = 16$ et $(RSB_1, RSB_2) = (20, 12)$ dB

plus complexe à implémenter.

On considère maintenant le cas du canal de diffusion avec message confidentiel. Soit αP la puissance utilisée pour les symboles de la constellation de l'information secrète avec $0 \leq \alpha \leq 1$. Les courbes des régions de débits atteignables montrent que le débit secret maximal n'est pas obtenu lorsque $\alpha = 1$, *i.e.* lorsque la puissance totale est dédiée à l'information secrète contrairement au cas du canal de diffusion sans contrainte de sécurité [37]. Cela montre que le débit secret n'augmente pas nécessairement avec le RSB des utilisateurs. Pour expliquer ce résultat, on va présenter les résultats pour le canal à écoute Gaussien où il n'y a pas de message commun à envoyer pour les récepteurs, i.e., lorsque $U = const.$ ($\theta = 1$). Cela va permettre de mieux comprendre le comportement des courbes des débits atteignables pour le canal de diffusion avec message confidentiel. Les conclusions obtenues ici sont aussi applicables en présence du message commun. La figure 3.12 montre le débit atteignable secret en utilisant des constellations M-PAM standard dont les symboles sont utilisés avec la même probabilité pour $M \in \{2, 4, 8, 16\}$, et la capacité secrète atteignable en utilisant un alphabet Gaussien, lorsque RSB_2 est plus petit que RSB_1 de 10 dB. Évidemment, le débit secret augmente quand l'écart entre RSB_1 et RSB_2 augmente pour RSB_1 fixé. Lorsque les RSB des deux récepteurs augmentent, le débit secret est nul, puisque $I(X;Y_1)$ et $I(X;Y_2)$ convergent vers $\log_2 M$. Par conséquent, le transmetteur doit augmenter la cardinalité M lorsque les RSBs augmentent afin de réduire l'écart avec la capacité secrète.

Dans la figure 3.13, le débit secret atteignable en utilisant un M-PAM est tracé en fonction du RSB_1 quand RSB_2 est fixé à 0 dB pour $M = 4, 8, 16$. Pour chaque valeur de M, le débit secret est calculé en utilisant une constellation standard (positions standard et probabilités égales des symboles) et comparé au cas dans lequel les positions des symboles et leurs probabilités sont optimisées. On observe que l'optimisation des positions des symboles et leurs probabilités conduit à des gains importants lorsque RSB_1 augmente avec RSB_2 fixé. En effet, quand RSB_1 augmente, $I(X;Y_1)$ tend vers $\log_2 M$. Ainsi, le débit secret $R_1 = I(X;Y_1) - I(X;Y_2)$ va tendre vers $\log_2 M - i_2$ où $i_2 = I(X;Y_2)$ quand l'alphabet d'entrée appartient à un M-PAM standard et lorsque le RSB est égal à 0

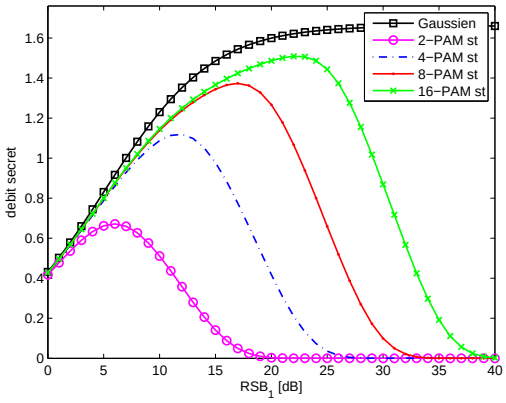

FIGURE 3.12 – Le débit secret pour un canal à écoute Gaussien en utilisant un alphabet Gaussien ou un M-PAM standard avec P_X uniforme. RSB_2 [dB]=RSB_1 [dB]-10 dB

dB. Cependant, lorsque les positions des symboles et la distribution P_X sont optimisées, l'émetteur peut ne pas utiliser la puissance moyenne maximale autorisée. Ainsi, lorsque RSB_1 augmente, l'émetteur peut utiliser une constellation dont les positions des symboles sont proches de l'origine tandis que $I(X;Y_1)$ atteint encore $\log_2 M$ puisque RSB_1 est très grand. Dans ce cas, $I(X;Y_2)$ va diminuer à cause de la petite valeur du RSB_2. Par conséquent, l'optimisation des positions des symboles et leurs probabilités permet au débit secret de converger vers une valeur proche de $\log_2 M$.

Une autre illustration est donnée dans la Fig. 3.14. La puissance de transmission optimale est représentée en fonction du RSB_1 lorsque RSB_2 est fixé à 0 dB et $M = 4$. On observe que lorsque $RSB_1 \leq 11$ dB, la puissance optimale est donnée par la puissance maximale autorisée $P = 5$. Cependant, lorsque $RSB_1 > 11$ dB, la puissance optimale diminue avec RSB_1.

On revient maintenant au cas de la superposition de modulation pour le canal de diffusion avec message confidentiel (et un message commun). Étudions par exemple le cas où RSB_1= 10 dB et $RSB_2 = 0$ dB. Les utilisateurs 1 et 2 reçoivent l'information secrète avec des rapports signal sur bruit $RSB'_1 = \alpha \cdot \frac{P}{\sigma_1^2}$ et $RSB'_2 = \alpha \cdot \frac{P}{\sigma_2^2}$ respectivement. Lorsque $\alpha = 1$, $RSB'_1 = 10$ dB et $RSB'_2 = 0$ dB, la capacité secrète est égale à 0.51

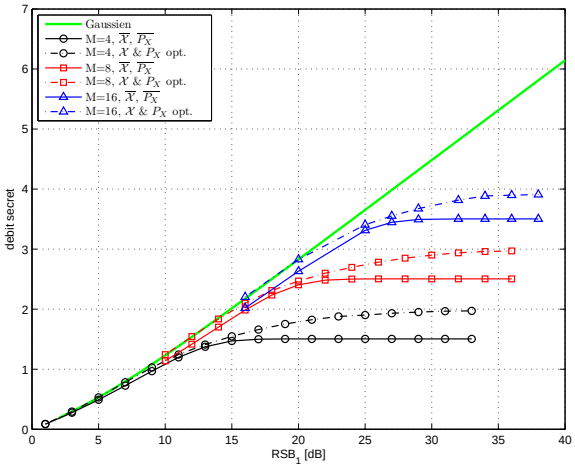

FIGURE 3.13 – schéma montrant le débit secret maximal pour un canal à écoute Gaussien en utilisant un M-PAM et en optimisant à la fois les positions des symboles et P_X et le débit en utilisant une constellation M-PAM standard en fonction du RSB_1. $RSB_2 = 0$ dB.

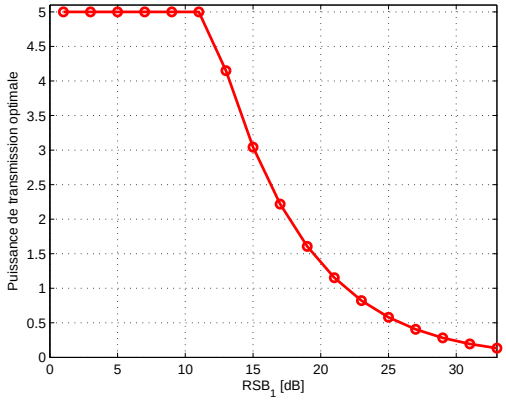

FIGURE 3.14 – Puissance de transmission optimale pour un canal à écoute Gaussien et $M = 4$ étant donné que la puissance maximale disponible est $P = 5$. $RSB_2 = 0$ dB.

bit/ch.use en utilisant une constellation 2-PAM selon la figure 3.12. On observe dans cette figure, que le débit secret maximal est obtenu quand $RSB_1 = 6$ dB ($RSB_2 = -4$ dB) et il est égal à 0.6711 bit/ch.use. Ainsi, la fraction de puissance optimale $\alpha = \alpha^*$ qui maximise le débit secret dans le cas du superposition de modulation est telle que $\alpha^* \cdot \frac{P}{\sigma_1^2} = 6$ dB. Évidemment, si on résout (3.8) on ne peut pas obtenir la région telle que $\alpha > \alpha^*$ car elle n'est pas optimale. C'est ce qu'on peut aussi observer des régions des débits atteignables en utilisant $\{8, 16\}$-PAM.

Time sharing ou superposition de modulation ?

La superposition de modulation avec symboles équiprobables et le *time sharing* avec des constellations standards sont largement utilisées comme stratégies de transmission pour les systèmes de diffusion par souci de simplicité. Les régions des débits atteignables en utilisant le *time sharing* ou la superposition de modulation peuvent être divisées en deux parties où le *time sharing* est meilleur que la superposition de modulation ou vice versa, selon les figures 3.4-3.11. La région des débits atteignables par la superposition de modulation devient de plus en plus importante relativement au *time sharing* lorsque l'écart entre les *RSB* des utilisateurs augmente. Par conséquent, la superposition de modulation doit être préférée au *time sharing* dans ce cas.

Codage par superposition

Les résultats obtenus pour le cas général du codage par superposition montrent que ce cas peut atteindre des débits meilleurs que la superposition de modulation ce qui signifie que la superposition de modulation n'est pas la stratégie de diffusion optimale comme dans le cas d'alphabet Gaussien. Les courbes des régions de débits atteignables (Fig. 3.4-3.11) montrent que le gain maximal en débits atteignables obtenu en utilisant le cas général du codage par superposition par rapport au superposition de modulation est plus grand pour les petites valeurs de M. Cela est dû au fait que lorsque M augmente, il existe plusieurs configurations pour obtenir un M-PAM en superposant deux constellations. Par exemple, lorsque $M = 8$ (Fig. 3.6 et Fig. 3.10) on a deux cas de superposition

de modulation. Asymptotiquement, on sait que lorsque $M \to \infty$, la superposition de modulation ($SM_{\mathcal{X},P_{UX},P_X}$) est la stratégie optimale puisqu'elle permet d'atteindre la région de capacité pour un canal de diffusion Gaussien en utilisant des alphabets Gaussiens (paragraphes 2.2.2 et 2.3.2). L'analyse des résultats obtenus montrent que dans certaines cas, la perte en débit par rapport au cas général du codage par superposition (la stratégie la plus complexe) peut être très petite en utilisant une stratégie plus simple que le cas général du codage par superposition [1].

Application : extension de la couverture

Tout d'abord, considérons une transmission sur un canal point-à-point où l'émetteur utilise une constellation standard dont les symboles sont utilisés avec des probabilités égales. L'utilisateur existant est à une distance d_0 de l'émetteur et atteint un débit R_0.

On suppose maintenant qu'on va transmettre de l'information vers une nouvelle couche d'utilisateurs sans contrainte de sécurité. On a étudié le cas où l'émetteur peut utiliser 16 symboles pour transmettre vers les deux couches d'utilisateurs. Par suite, plusieurs stratégies de transmission peuvent être utilisées. L'objectif est de comparer les stratégies de transmission pour servir la nouvelle couche d'utilisateurs dans deux scénarios : le premier est lorsque la nouvelle couche d'utilisateurs est plus proche de l'émetteur que la couche existante initialement et le deuxième lorsque la nouvelle couche est plus loin que celle qui existe initialement. Pour un débit R_0 cible qui est fixé pour les utilisateurs initiaux en utilisant une constellation M-PAM standard et des symboles équiprobables, on souhaite déterminer la variation du rapport de diamètre de couverture des deux couches d'utilisateurs en fonction du débit atteignable par la nouvelle couche d'utilisateurs pour différentes stratégies de transmission.

Les résultats sont détaillés dans l'annexe A. Ils montrent que l'optimisation de la distribution de probabilité jointe dans le cas de la superposition de modulation est souvent utile et fournit des gains remarquables. L'utilisation du codage par superposition peut apporter des gains significatifs par rapport au cas du superposition de modulation selon le diamètre de la zone de couverture de la nouvelle couche d'utilisateurs.

Dans une autre expérience, on a étudié ces deux scénarios avec la contrainte que la cardinalité de l'alphabet des utilisateurs initiales reste fixe après l'introduction de la nouvelle couche des utilisateurs [1].

3.5.3 Quel est l'impact de la contrainte de sécurité ?

Tout d'abord, on rappelle que la région de capacité d'un canal de diffusion Gaussien avec deux utilisateurs et une contrainte de puissance, sans contrainte de sécurité, telle que $RSB_1 > RSB_2$ est :

$$R_0 \leq \frac{1}{2}\log_2\left(1+\frac{(1-\beta)\cdot P}{N_2+\beta\cdot P}\right) \tag{3.14}$$

$$R_{p1} \leq \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_1}\right) \tag{3.15}$$

où R_0 est le débit du message commun pour les deux récepteurs et R_{p1} est le débit du message privé dédié à l'utilisateur 1. Dans le cas du canal de diffusion avec message confidentiel, le débit du message confidentiel pour l'utilisateur 1, R_1 est tel que

$$R_1 \leq \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_1}\right) - \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_2}\right) \tag{3.16}$$

On observe qu'il y a un "écart de confidentialité" égal à $R' = \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_2}\right)$ entre le débit du message privé pour l'utilisateur 1 et le débit secret R_1. Donc, on peut transmettre un message privé à l'utilisateur 1 avec un débit R_{p1} ; cependant, seulement une portion de ce message de débit R_1 peut être sécurisée. Par conséquent, il est possible de transmettre à l'utilisateur 1 deux messages avec un débit total égal à R_{p1} : un message secret avec un débit R_1 et un message privé sans garantie de sécurité avec un débit R'. La figure 3.15 montre en même temps la région de capacité (R_0 vs R_{p1}) et la région de capacité secrète (R_0 vs R_1) pour plusieurs paires des RSB et pour $M = 4, 8, 16$. Pour un RSB_1 fixé, cet écart de confidentialité augmente lorsque RSB_2. Pour le cas de l'alphabet fini, et en utilisant le cas général du codage par superposition, on observe que l'écart de confidentialité entre le débit maximal du message privé et le débit maximal secret pour un R_0 fixé est proche que celui obtenu dans le cas de l'alphabet Gaussien pour les paires

RSBs étudiées. Cependant, lorsque RSB_1 augmente, R_{p1} tend vers $\log_2 M$ et donc l'écart dans le cas de l'alphabet fini devient plus petit que dans le cas de l'alphabet Gaussien. C'est ce qu'on peut observer dans la figure 3.15 pour la stratégie du superposition de modulation utilisant des symboles équiprobables et avec une constellation 4-PAM, où la valeur maximale de R_{p1} est égale à 1 (la valeur maximale possible en utilisant un 2-PAM). Ainsi, l'écart de confidentialité entre la régions des débits atteignables maximales avec et sans contrainte de sécurité est plus petit que dans le cas d'alphabet Gaussien ou dans le cas général du codage par superposition pour les paires RSBs étudiées.

3.6 Conclusion

Dans ce chapitre, on a étudié le problème de maximisation de la région des débits atteignables sous une contrainte de puissance pour un canal de diffusion Gaussien avec deux utilisateurs en utilisant des constellations M-PAM. Deux types de canaux de diffusion sont étudiés : le premier est lorsque l'émetteur a un message commun pour les deux récepteurs et un message privé pour l'un d'eux et le deuxième cas est le canal de diffusion avec message confidentiel et un message commun. La région des débits atteignables a été donnée pour plusieurs stratégies de transmission. Les différentes stratégies sont comparées en termes d'efficacité en débits atteignables tout en analysant le compromis entre l'efficacité et la complexité d'implémentation de ces stratégies. On a observé que la puissance de transmission optimale qui maximise le débit secret vers l'un des deux utilisateurs n'est pas nécessairement égale à la puissance maximale disponible chez l'émetteur (contrairement au cas sans contrainte de sécurité). On a observé aussi que la contrainte d'alphabet fini peut changer des résultats bien connus pour le cas d'alphabet Gaussien. La superposition de modulation n'est pas la stratégie optimale dans le cas d'alphabet fini contrairement au cas d'alphabet Gaussien. L'analyse des résultats montrent aussi que les stratégies les plus complexes (comme le cas général du codage par superposition) apportent parfois des gains significatifs par rapport aux stratégies les plus simples. Cependant, dans d'autres cas, l'utilisation des stratégies pratiques est suffisant

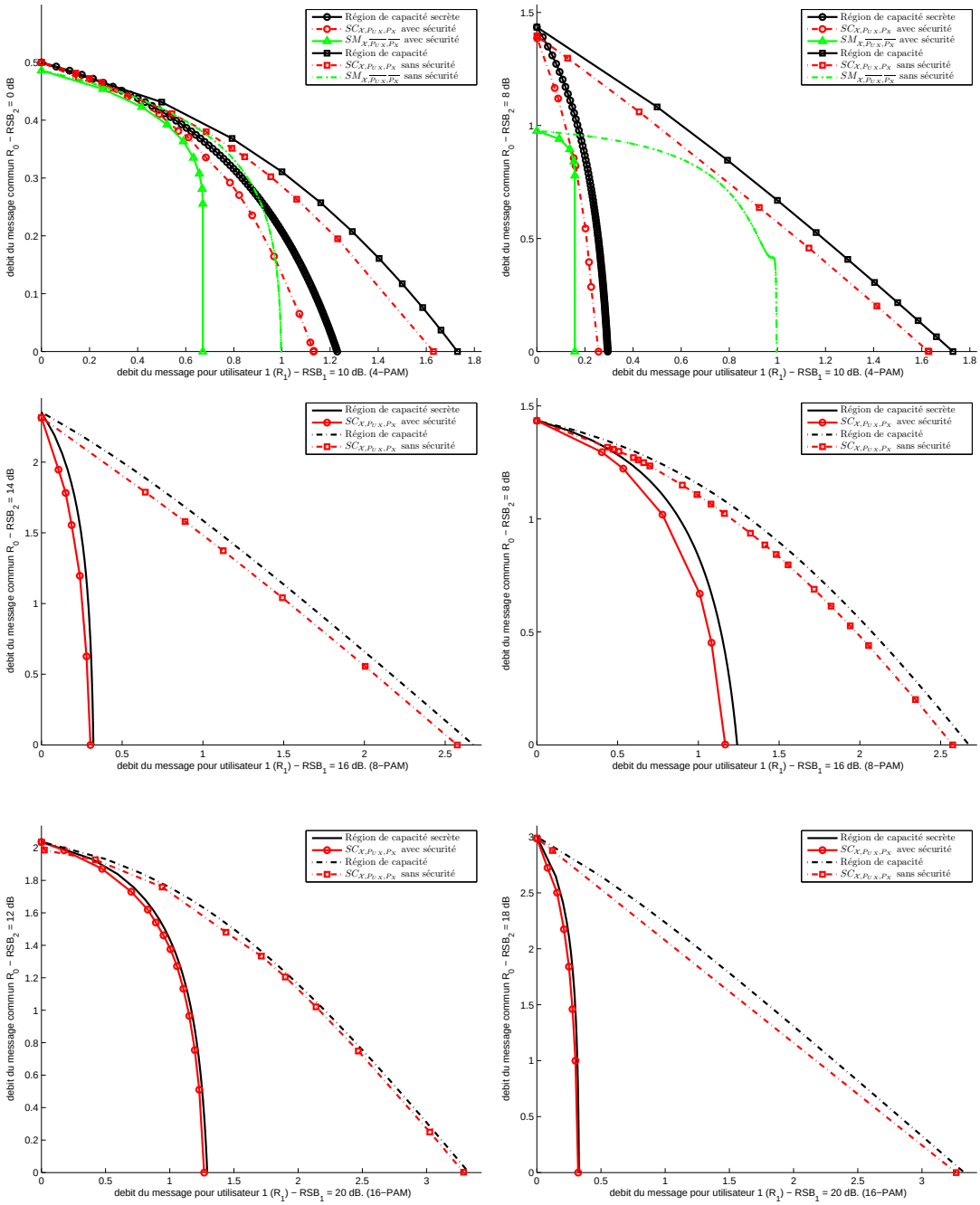

FIGURE 3.15 – Débits atteignables maximales pour un canal de diffusion avec alphabet fini ou Gaussien / avec ou sans la contrainte de sécurité.

pour obtenir de bons débits et fournit un compromis entre l'implémentation pratique et l'efficacité en débits atteignables. Finalement, on a analysé l'impact de la contrainte de sécurité et on observé que l'écart de confidentialité pour confondre l'espion peut être important selon les rapports signal sur bruit des utilisateurs.

Chapitre 4

Adaptation du débit pour les protocoles HARQ sécurisés avec redondance incrémentale

Sommaire

4.1 Introduction

La capacité secrète a été étudiée dans [11], [12] pour les canaux à écoute à évanouissement avec une hypothèse d'une connaissance parfaite de l'état instantané du canal. Dans ce

chapitre, on considère le canal à écoute à évanouissement par blocs lorsque l'émetteur n'a pas une information sur l'état instantané du canal, mais connait seulement les statistiques. On va étudier un schéma appelé HARQ avec "redondance incrémentale" où plusieurs ensembles de bits codés sont générés et utilisés dans les retransmissions, représentant chacun le même bloc de données. Plus précisément, dans ce schéma, le message est codé par le transmetteur par un code "mère". Initialement, seulement un certain nombre de symboles codés sont transmis. Ce nombre de symboles codés forme un code poinçonné. Lorsqu'une retransmission est demandée, des symboles de redondance additionnels sont transmis. Des travaux sur l'analyse des codes "mères" et leurs poinçonnages sont présentés dans [71]–[76]. Le travail présenté dans cette partie est inspiré de celui dans [48] où les auteurs ont fait une étude basée sur la théorie d'information des protocoles HARQ pour un canal à écoute à évanouissement par blocs. A cause de l'absence de l'information sur l'état instantané du canal, l'émetteur ne peut pas adapter les débits aux conditions instantanées du canal. Dans le modèle de système de [48], l'émetteur obtient un feedback de 1-bit ACK/NACK du récepteur légitime pour déclarer une réussite/échec du décodage par un canal public sans erreur. Les auteurs considèrent aussi un schéma de redondance incrémentale dans lequel les sous-mots de code ont la même longueur dans chaque retransmission. Dans ce travail, on va généraliser les hypothèses de [48] en considérant des canaux de retour à niveaux multiples du récepteur légitime et de l'espion à la fois. Par suite, la longueur des sous-mots de code est adaptée à chaque retransmission en utilisant les canaux de retour afin de maximiser le débit utile secret sous contraintes d'*outages*. On comparera le schéma adaptatif à débit variable dans chaque retransmission conçu dans ce chapitre au schéma non-adaptatif à débit fixe dans [48]. En effet, les gains de transmission à débit variable par rapport au débit fixe pour les familles de code prédéfinies ont été vérifiés dans de nombreux travaux comme [77], [78], [79].

Les détails des calculs de ce chapitre se trouvent dans le rapport technique joint dans l'annexe C.

4.2 Modèle du système

On considère le canal à écoute à évanouissement par blocs dans lequel un émetteur X envoie des messages confidentiels à un récepteur légitime Y en présence d'un espion Z écoutant la transmission (Figure 4.1). Les canaux vers le récepteur légitime et l'espion subissent un évanouissement par K blocs où les canaux restent constants dans un bloc mais varient indépendamment d'un bloc à un autre [80]. Chez l'émetteur, un message confidentiel w est codé en un mot de code x^N de N symboles $x_1, x_2, .., x_N$. La longueur N du mot de code n'est pas fixée, càd on suppose que le code peut être construit avec un taux arbitraire comme dans [77]. Un sous-ensemble des symboles x_j est appelé un sous-mot de code. Le mot de code x^N est divisé en K sous-mots de code $\mathbf{x}_k$, $k = 1, .., K$. Le mot de code occupe K intervalles de temps. Le $k^{\text{ème}}$ bloc $\mathbf{x}_k$ est envoyé dans le $k^{\text{ème}}$ intervalle de temps et reçu par le récepteur légitime et l'espion avec des gains de canal $\sqrt{h_k}$ et $\sqrt{g_k}$ respectivement, pour $k = 1, .., K$.

Les expressions des symboles y_t et z_t reçus par le récepteur légitime et l'espion respectivement, après l'envoi du $t^{\text{ème}}$ symbole x_t par l'émetteur dans le $k^{\text{ème}}$ bloc, sont les suivantes.

$$y_t = \sqrt{h_k} \cdot x_t + v_t \tag{4.1}$$

$$z_t = \sqrt{g_k} \cdot x_t + u_t \tag{4.2}$$

où k indique le numéro du bloc, $t = 1, .., N$ est l'indice du symbole transmis, v_t et u_t sont des bruits Gaussiens i.i.d. avec une moyenne nulle et une variance unitaire.

On suppose que l'entrée du canal X suit une distribution Gaussienne réelle avec une moyenne nulle et une variance unitaire ($\mathbb{E}[X^2] \leq 1$). Ainsi, les rapport signal sur bruit reçus chez le récepteur légitime et l'espion sont respectivement h_k et g_k durant la $k^{\text{ème}}$ transmission. On suppose aussi que l'émetteur n'a aucune information sur l'état instantané des canaux du récepteur légitime et de l'espion. L'émetteur connait seulement les statistiques de ces canaux. Par contre, le récepteur légitime et l'espion connaissent chacun le gain de leur propre canal dans chaque bloc.

Dans ce qui suit, on considère un évanouissement de Rayleigh. Par conséquent, le

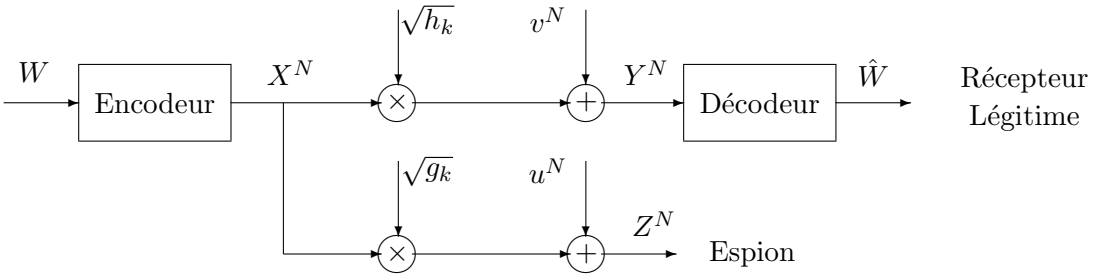

FIGURE 4.1 – Canal à écoute à évanouissement

RSB instantané du canal du récepteur légitime h et le *RSB* instantané du canal de l'espion g sont caractérisés par des distributions de probabilités exponentielles :

$$p_H(x) = \frac{1}{\overline{h}} \cdot e^{-\frac{x}{\overline{h}}} \tag{4.3}$$

$$p_G(x) = \frac{1}{\overline{g}} \cdot e^{-\frac{x}{\overline{g}}} \tag{4.4}$$

où $\overline{h}$ et $\overline{g}$ sont les *RSB*s moyens du canal de légitime et celui de l'espion respectivement.

Afin d'introduire les codes de Wyner pour le canal à écoute qui constituent la base des protocoles HARQ sécurisés dans ce chapitre, considérons le cas particulier d'une transmission avec un seul bloc (i.e. $K = 1$). Soit $C(N, R, R_s)$ le code Wyner utilisé pour transmettre l'ensemble de messages confidentiels $\mathcal{W} = \{1, 2, .., 2^{NR_s}\}$ où N est la longueur du mot de code, R est le débit de code du canal du légitime et R_s ($R_s \leq R$) est le débit de l'information secrète. L'idée principale des codes de Wyner est l'utilisation d'un codeur stochastique pour augmenter le niveau de sécurité [7]. Le code de Wyner est construit en basant sur le *random binning* de la façon suivante. On génère tout d'abord 2^{NR} mots de code $x^N(w, v)$, où $w = 1, 2, .., 2^{NR_s}$ et $v = 1, 2, .., 2^{N(R-R_s)}$, en choisissant les $N2^{NR}$ symboles $x_i(w, v)$ indépendamment et aléatoirement selon la distribution $p(x)$. Pour coder le message $w \in \mathcal{W}$, on sélectionne uniformément au hasard v de $\{1, 2, .., 2^{N(R-R_s)}\}$ et on transmet $x^N = x^N(w, v)$. La paire de débits atteignables

(R, R_s) satisfait [48] :

$$R \leq I(X;Y) \tag{4.5}$$

$$R - R_s \geq I(X;Z) \tag{4.6}$$

Dans ce qui suit, on utilise les notations $M_i = N \cdot R_s$ pour désigner le nombre de bits d'information (qui est fixé) et $M_T = N \cdot R$ pour désigner le nombre total de bits transmis incluant M_d bits "fictifs". Le débit correspondant $R' = R - R_s$ est le débit nécessaire pour assurer la sécurité.

Le codebook est révélé à tous les nœuds. On suppose qu'un codage aléatoire permettant d'atteindre la capacité est utilisé et que les récepteurs implémentent le décodage typique qui nous permet de trouver les limites de performance pour n'importe quel schéma pratique.

4.3 Formulation du problème

On considère que le HARQ sécurisé avec redondance incrémentale est utilisé comme un protocole de transmission. Les N symboles du mot de code sont divisés en K sous-mots de code $\mathbf{x_k}$, $k = 1, .., K$ chacun de longueur N_k (Les sous-mots de code peuvent avoir des longueurs différentes) où $N = \sum_{k=1}^{K} N_k$. On définit le rapport des bits secrets transmis par $\gamma = \frac{M_i}{M_T} = \frac{M_i}{M_i + M_d}$. Le nombre de bits fictifs M_d est choisi par l'émetteur selon les statistiques des canaux. Le processus ARQ commence par l'envoi du premier sous-mot de code $\mathbf{x}_1$ telle que la paire des RSBs est (h_1, g_1). Ensuite le décodage est fait chez le récepteur légitime et le niveau de sécurité est mesuré chez l'espion. Si le décodage n'est pas réussi ; une seconde retransmission est demandée par le récepteur légitime et le second sous-mot de code $\mathbf{x}_2$ est émis éventuellement avec des conditions différentes (h_2, g_2). Ensuite, le décodage chez le légitime et le calcul du niveau de sécurité chez l'espion sont effectués en combinant le bloc précédant $\mathbf{x}_1$ avec le nouveau bloc $\mathbf{x}_2$. Cela continue jusqu'à ce que le nombre maximal des transmissions K soit atteint ou si le décodage est réussi chez le récepteur légitime.

Puisque l'émetteur n'a aucune information sur l'état instantané du canal, les débits ne peuvent pas être choisis pour un état particulier du canal à évanouissement. Au lieu de çà, un code Wyner fixé à l'avance est utilisé pour toutes les conditions du canal.

4.3.1 Schéma adaptatif de la redondance incrémentale

Dans ce travail, on considère un modèle général dans lequel l'émetteur utilise des canaux de retour à niveaux multiples (*multi-level feedback*) sans erreur du récepteur légitime et de l'espion à la fois. De plus, on considère que les sous-mots de code $\mathbf{x_k}$ peuvent avoir des longueurs différentes. Après k transmissions, chaque récepteur applique le décodage de maximum de vraisemblance en utilisant les observations du canal obtenues jusqu'à la $k^{\text{ème}}$ transmission.

La condition d'un décodage réussi chez le récepteur légitime après k transmissions est telle que la moyenne de l'information mutuelle accumulée est plus grande que le débit de code $R = \frac{M_T}{N}$. Cette condition est donnée pour le cas d'une transmission avec un seul bloc dans (4.5). Dans le modèle considéré, dans lequel les sous-mots de codes $\mathbf{x_k}$ peuvent avoir des longueurs différents, cette condition peut être écrite comme :

$$\frac{M_T}{\sum_{l=1}^{k} N_l} \leq \frac{\sum_{l=1}^{k} c_l^{\mathcal{D}} \cdot N_l}{\sum_{l=1}^{k} N_l} \tag{4.7}$$

où N_l est la longueur du sous-mot de code émis durant la $l^{\text{ème}}$ transmission et $c_l^{\mathcal{D}} = I(X;Y|h_l)$ est l'information mutuelle entre l'entrée X et la sortie Y d'un canal point-à-point avec un rapport signal-sur-bruit égal à h_l. Puisqu'on a considéré un alphabet d'entrée gaussien, on a $c_l^{\mathcal{D}} = \frac{1}{2}\log_2(1 + h_l)$. Pour des raisons pratiques, on normalise les valeurs de N_l et on utilisera la notation $\rho_l = \frac{N_l}{M_T}$ qui est interprété comme la "redondance" apportée par le $l^{\text{ème}}$ sous-mot de code. Par conséquent, (4.7) s'écrit :

$$I_k^{\mathcal{D}} \stackrel{\triangle}{=} \sum_{l=1}^{k} c_l^{\mathcal{D}} \cdot \rho_l \geq 1 \tag{4.8}$$

On appellera $I_k^{\mathcal{D}}$ "l'état du décodeur" chez le récepteur légitime (D).

La condition de sécurité chez l'espion après k transmissions, donnée dans (4.6) pour le cas d'une transmission avec un seul bloc, est telle que la moyenne de l'information

mutuelle accumulée est plus petite que la différence entre le débit de code R et le débit de l'information secrète $R_s = \frac{M_i}{N}$:

$$\frac{M_T}{\sum_{l=1}^{k} N_l} - \frac{M_i}{\sum_{l=1}^{k} N_l} \geq \frac{\sum_{l=1}^{k} c_l^{\mathcal{E}} \cdot N_l}{\sum_{l=1}^{k} N_l} \tag{4.9}$$

ce qui est équivalent à,

$$I_k^{\mathcal{E}} \stackrel{\triangle}{=} \sum_{l=1}^{k} c_l^{\mathcal{E}} \cdot \rho_l + \gamma \leq 1 \tag{4.10}$$

où $c_l^{\mathcal{E}} = I(X; Z|g_l) = \frac{1}{2}\log_2(1 + g_l)$.

A partir des équations (4.8) et (4.10), on sait que les événements des erreurs du décodage dans la $k^{\text{ème}}$ transmission chez le récepteur légitime et l'espion dépendent de $I_{k-1}^{\mathcal{D}}$ et $I_{k-1}^{\mathcal{E}}$, qui sont communiqués à l'émetteur par l'intermédiaire des canaux de retour, et de $c_k^{\mathcal{D}}$ et $c_k^{\mathcal{E}}$, qui sont inconnus à l'émetteur et qui ne peuvent pas être prédits en utilisant les états précédents en raison de l'hypothèse des gains des canaux i.i.d. . Par conséquence, $I_{k-1}^{\mathcal{D}}$ et $I_{k-1}^{\mathcal{E}}$ sont les seuls paramètres que l'émetteur peut utiliser pour adapter les ρ_k. On considère alors la "politique" suivante pour la tentative de transmission numéro k :

$$\rho_k = \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}), \quad k = 1, ..., K \tag{4.11}$$

où

$$\rho_k = \begin{cases} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) & \text{si } I_{k-1}^{\mathcal{D}} < 1 \text{ et } I_{k-1}^{\mathcal{E}} \leq 1 \\ \rho_k(I_{k-1}^{\mathcal{D}}) & \text{si } I_{k-1}^{\mathcal{D}} < 1 \text{ et } I_{k-1}^{\mathcal{E}} > 1 \\ 0 & \text{autrement.} \end{cases} \tag{4.12}$$

Cela fait la différence avec le travail fait dans [48] qui considère le cas particulier lorsque $\rho_k = \rho \ \forall k$. Le but est de trouver les politiques d'adaptation des ρ_k, pour toutes les valeurs du couple $(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})$ représentant les informations transmises par les canaux de retour, et aussi du γ qui optimisent un certain critère de performance défini dans le paragraphe suivant. Par souci de simplicité, on néglige les erreurs de transmission et de discrétisation pour les canaux de retour et on suppose que l'émetteur connait parfaitement $I_{k-1}^{\mathcal{D}}$ et $I_{k-1}^{\mathcal{E}}$.

4.3.2 Expression du débit utile secret

Le critère de performance pertinent afin d'évaluer les protocoles HARQ sécurisés est le débit utile secret. L'objectif est donc de trouver les ρ_k (qui sont des fonctions de deux variables) et le γ qui maximisent le débit utile secret atteignable pour le système considéré. En basant sur le théorème du reward-renewal [45],[44], le débit utile secret est défini par le rapport entre le nombre des bits d'information reçus d'une manière fiable à la dernière transmission par le récepteur légitime M_i^* et l'espérance du nombre des utilisations du canal (ou symboles) $\overline{N}$ requis par le protocole HARQ pour délivrer le paquet jusqu'au K tentatives de transmission maximum :

$$\eta = \frac{M_i^*}{\overline{N}} \tag{4.13}$$

Le débit utile secret est un critère de performance pertinent puisqu'il peut être lié directement à la capacité secrète du canal [45], [47]. Comme l'émetteur ne connait pas l'état instantané du canal à écoute, il ne peut pas adapter le débit selon les conditions instantanées du canal. Pour cela, on va considérer la performance du protocole HARQ sécurisé sous des contraintes d'*outages*. En effet, on considère que la qualité de service est acceptable tant que le pourcentage maximal des bits d'information qui ne sont pas décodés correctement par le récepteur légitime est plus petit que ξ_e et que le pourcentage maximal des bits d'information décodés correctement par l'espion dans la dernière transmission est plus petit que ξ_s. Pour cela, on définit la probabilité du "*connection outage*" f_0 par la probabilité d'un décodage non-réussi après K transmissions chez le récepteur légitime et la probabilité d'un "*secure outage*" f_s par la probabilité d'un décodage réussi chez l'espion dans la dernière transmission. Ces probabilités d'*outages* sont utilisées pour caractériser le compromis entre la fiabilité des transmissions sur le canal du récepteur légitime et la confidentialité chez l'espion.

- $M_i^* = M_i \cdot (1 - f_0)$, où f_0 peut être écrite de la manière suivante :

$$f_0 = \Pr\{I_K^{\mathcal{D}} < 1\} = \mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}}\{\mathbb{I}(I_K^{\mathcal{D}} < 1)\} = \int_0^1 dx \int_\gamma^\infty dy \; p_{I_K^{\mathcal{D}} \; I_K^{\mathcal{E}}}(x, y) \tag{4.14}$$

où $\mathbb{I}(x) = 1$ si x est vraie et $\mathbb{I}(x) = 0$ si x est faux. $p_{I_K^{\mathcal{D}} \; I_K^{\mathcal{E}}}(x, y)$ est la densité jointe de $I_K^{\mathcal{D}}$ et $I_K^{\mathcal{E}}$.

– L'espérance du nombre des utilisations du canal est donnée par $\overline{N} = \sum_{k=1}^{K} \overline{N}_k$, où $\overline{N}_k$ est l'espérance du nombre des utilisations du canal dans la $k^{\text{ème}}$ transmission :

$$\overline{N}_k = M_T \cdot \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}}\{\rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1})\} = M_T \cdot \int_0^1 dx \int_\gamma^\infty dy \; \rho_k(x,y) \cdot p_{I^{\mathcal{D}}_{k-1} \; I^{\mathcal{E}}_{k-1}}(x,y)$$

Alors l'expression du débit utile secret est la suivante :

$$\eta = \gamma \cdot \frac{1 - f_0}{\sum_{k=1}^{K} \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}}\{\rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1})\}} \tag{4.15}$$

Soit $\mathcal{K}$ le nombre de transmission dans une session HARQ (ou le numéro de la dernière transmission). La probabilité du *secrecy outage* f_s s'écrit donc :

$$\begin{aligned} f_s &= \Pr(I^{\mathcal{E}}_{\mathcal{K}} > 1) && (4.16)\\ &= \sum_{k=1}^{K} \Pr(I^{\mathcal{E}}_{\mathcal{K}} > 1, \mathcal{K} = k) && (4.17)\\ &= \sum_{k=1}^{K} \Pr(\mathcal{K} = k) \cdot \Pr(I^{\mathcal{E}}_{\mathcal{K}} > 1 | \mathcal{K} = k) && (4.18)\\ &= \sum_{k=1}^{K} \Pr(\mathcal{K} = k) \cdot \Pr(I^{\mathcal{E}}_{k} > 1) && (4.19) \end{aligned}$$

où :

– La fonction de masse de $\mathcal{K}$ est :

$$\begin{aligned} \Pr(\mathcal{K} = k) &= \Pr(I^{\mathcal{D}}_{k-1} < 1, I^{\mathcal{D}}_{k} \geq 1) \\ &= \Pr(I^{\mathcal{D}}_{k-1} < 1) - \Pr(I^{\mathcal{D}}_{k-1} < 1, I^{\mathcal{D}}_{k} < 1) \\ &= \Pr(I^{\mathcal{D}}_{k-1} < 1) - \Pr(I^{\mathcal{D}}_{k} < 1) \\ &= \mathbb{E}_{C^{\mathcal{D}}_1, .., C^{\mathcal{D}}_{k-1}}\{\mathbb{I}(I^{\mathcal{D}}_{k-1} < 1)\} - \mathbb{E}_{C^{\mathcal{D}}_1, .., C^{\mathcal{D}}_{k}}\{\mathbb{I}(I^{\mathcal{D}}_{k} < 1)\} \end{aligned}$$

pour $k < K$ et

$$\Pr(\mathcal{K} = K) = \Pr(I^{\mathcal{D}}_{K-1} < 1) = \mathbb{E}_{C^{\mathcal{D}}_1, .., C^{\mathcal{D}}_{K-1}}\{\mathbb{I}(I^{\mathcal{D}}_{K-1} < 1)\}$$

– La probabilité que l'espion décode le message confidentiel dans la $k^{\text{ème}}$ transmission s'écrit :

$$\Pr(I_k^{\mathcal{E}} > 1) = \mathbb{E}_{C_1^{\mathcal{E}},..,C_k^{\mathcal{E}}}\{\mathbb{I}(I_k^{\mathcal{E}} > 1)\} = \int_0^{\infty} dx \int_1^{\infty} dy \; p_{I_k^{\mathcal{D}} \; I_k^{\mathcal{E}}}(x, y) \tag{4.20}$$

Le débit utile secret (4.15) dépend du modèle du canal et des schéma de codage et de décodage. Ici, on a supposé que le schéma du codage/décodage atteint la capacité comme dans [45] ce qui permet d'avoir la limite de performance de n'importe quel schéma pratique.

4.4 Problème de maximisation du débit utile secret sous contraintes

Le problème d'optimisation du débit utile secret sous contraintes d'*outages* est formulé par :

$$\max_{\gamma,\rho_1,...,\rho_K} \quad \eta(\rho_1, ..., \rho_K, \gamma)$$
$$s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases} \tag{4.21}$$

où ξ_ϵ et ξ_s sont les probabilités d'*outage* cibles. On rappelle ci-après les expressions des variables d'optimisation $\gamma, \rho_1, ..., \rho_K$:

– $\gamma = \frac{M_i}{M_i+M_d}$; où M_i, qui est le nombre de bits d'information, est une quantité fixée à l'émetteur et M_d, qui est le nombre de bits additionnels pour assurer la sécurité, est une variable d'optimisation.

– $\rho_k = \frac{N_k}{M_i+M_d}$ et $k \in \{1, .., K\}$. N_k, qui représente la longueur du sous mot de code envoyé dans le bloc numéro k, est une variable d'optimisation. Les $\rho_1, ..., \rho_K$ sont des fonctions bidimensionnelles : $\rho_k = \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})$ pour $k = 1, .., K$. On rappelle que $I_{k-1}^{\mathcal{D}}$ et $I_{k-1}^{\mathcal{E}}$ sont les quantités communiquées à l'émetteur par l'intermédiaire des canaux de retour du récepteur légitime et de l'espion respectivement. Les ρ_k (par suite les N_k) seront optimisés pour toutes les valeurs possibles de $I_{k-1}^{\mathcal{D}}$ et $I_{k-1}^{\mathcal{E}}$, avec $k \in \{1, .., K\}$.

On rappelle aussi que les expressions des probabilités d'*outages* f_0 et f_s sont les suivantes, d'après (4.14) et (4.19),

$$
\begin{aligned}
f_0 &= \mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}}\{\mathbb{I}(I_K^{\mathcal{D}} < 1)\} \text{ et} \\
f_s &= \sum_{k=1}^{K-1} \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}} \left\{ \mathbb{I}(I_{k-1}^{\mathcal{D}} < 1) - \mathbb{I}(I_k^{\mathcal{D}} < 1) \right\} \cdot \mathbb{E}_{C_1^{\mathcal{E}},..,C_k^{\mathcal{E}}} \left\{ \mathbb{I}(I_k^{\mathcal{E}} > 1) \right\} \right] \\
&+ \quad \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}} \left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \mathbb{E}_{C_1^{\mathcal{E}},..,C_K^{\mathcal{E}}} \left\{ \mathbb{I}(I_K^{\mathcal{E}} > 1) \right\} \right]
\end{aligned}
$$

4.5 Algorithme d'optimisation du débit utile secret sous contraintes

La conception du schéma du HARQ adaptatif avec redondance incrémentale consiste à trouver les politiques d'adaptation des ρ_k, $k = 1, ..., K$ et du γ qui maximisent le débit utile secret sous des contraintes sur les probabilités d'*outages* en ayant comme hypothèse que l'émetteur connait seulement les statistiques des canaux du récepteur légitime et de l'espion.

Dans cette section, on décrit brièvement l'algorithme utilisé pour résoudre le problème (4.21). Cet algorithme est détaillé dans l'annexe C.

Tout d'abord, pour trouver le γ optimal qui maximise le débit utile secret, on va utiliser la méthode de recherche exhaustive. Pour cela, on a résolu le problème (4.21) pour plusieurs valeurs de $\gamma \in [0, 1]$. Une fois $\gamma \in [0, 1]$ est fixé, la maximisation du débit utile secret serait par rapport aux ρ_k seulement et le problème d'optimisation s'écrit comme suit :

$$
\begin{aligned}
&\max_{\rho_1,...,\rho_K} \quad \eta(\rho_1, ..., \rho_K; \gamma) \\
&s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases}
\end{aligned} \tag{4.22}
$$

On discutera, à la fin de ce paragraphe, la méthode pour choisir les bonnes valeurs de γ. Maintenant, on suppose que γ est fixé à une valeur arbitraire dans $[0, 1]$. Dans ce qui suit, on explique la méthode de résolution du problème (4.22) en utilisant la programmation

dynamique. Pour maximiser le débit utile secret η dans le problème (4.22), on va définir un problème d'optimisation auxiliaire :

$$U(\xi_\epsilon, \xi_s) = \min_{\rho_1,\ldots,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}} \left\{ \rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) \right\} \quad \text{s.t.} \quad f_0 = \xi_\epsilon \quad \text{et} \quad f_s = \xi_s \tag{4.23}$$

Le débit utile secret maximal est obtenu en résolvant :

$$\hat{\eta} = \max_{\xi_\epsilon, \xi_s} \frac{1-\xi_\epsilon}{U(\xi_\epsilon, \xi_s)} = \frac{1-\hat{\xi}_\epsilon}{U(\hat{\xi}_\epsilon, \hat{\xi}_s)} \tag{4.24}$$

et la maximisation du débit utile secret sous contraintes d'*outages* $\hat{\eta}_{\epsilon s}$

$$\hat{\eta}_{\epsilon s} = \max_{\rho_1,\ldots,\rho_K} \eta, \quad \text{s.t.} \quad f_0 \leq \xi_\epsilon \quad \text{et} \quad f_s \leq \xi_s$$

est obtenue par

$$\hat{\eta}_{\epsilon s} = \begin{cases} \hat{\eta} & \text{si } \hat{\xi}_\epsilon < \xi_\epsilon \quad \text{et } \hat{\xi}_s < \xi_s \\ \\ \gamma \cdot \frac{1-\xi_\epsilon}{U(\xi_\epsilon, \xi_s)} & \text{autrement.} \end{cases}$$

Ainsi, la conception des politiques d'adaptation du débit exige la résolution de (4.23) qui peut être faite en utilisant des multiplicateurs λ_1 et λ_2 :

$$\begin{aligned} U(\xi_\epsilon, \xi_s) = \min_{\rho_1,\ldots,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}} \left\{ \rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) \right\} + \lambda_1 \cdot (f_0 - \xi_\epsilon) + \lambda_2 \cdot (f_s - \xi_s) \\ \text{s.t.} \quad \lambda_1 \cdot (f_0 - \xi_\epsilon) = 0 \quad \text{et} \quad \lambda_2 \cdot (f_s - \xi_s) = 0 \end{aligned} \tag{4.25}$$

On est intéressé par l'évaluation de $U(\xi_\epsilon, \xi_s)$ pour plusieurs valeurs de ξ_ϵ et ξ_s. Puisque pour chaque couple de λ_1 et λ_2 correspond un *connection outage* f_0 et un *secrecy outage* f_s, on peut résoudre (4.25) pour plusieurs valeurs de λ_1 et λ_2. Par suite, pour résoudre (4.15) on utilise des multiplicateurs auxiliaires λ_1 et λ_2 et on minimise le dénominateur de (4.15), f_0 et f_s en même temps :

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,\ldots,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}} \left\{ \rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) \right\} + \lambda_1 \cdot f_0(\rho_1, ..., \rho_K) + \lambda_2 \cdot f_s(\rho_1, ..., \rho_K) \tag{4.26}$$

Étape 0	$\lambda_1 \leftarrow \lambda_1^{(0)}$, $\lambda_2 \leftarrow \lambda_2^{(0)}$
Étape ℓ	1. résoudre $J^{\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)}}$ dans (4.27) 2. calculer les fonctions de probabilités jointes dans (4.35) et (4.39) pour $k = 1, .., K$ 3. calculer l'*outage* $f_0^{(\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)})}$ en utilisant (4.14). 4. mis à jour de λ_1 : $\lambda_1^{(\ell)} = [\lambda_1^{(\ell-1)} + \beta(f_0^{(\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)})} - \xi_0)]^+$ où $[.]^+ = \max(., 0)$
	1. résoudre $J^{\lambda_1^{(\ell)},\lambda_2^{(\ell-1)}}$ dans (4.27) 2. calculer les fonctions de probabilités jointes dans (4.35) and (4.39) pour $k = 1, .., K$ 3. calculer l'*outage* $f_s^{(\lambda_1^{(\ell)},\lambda_2^{(\ell-1)})}$ en utilisant (4.19). 4. mis à jour de λ_2 : $\lambda_2^{(\ell)} = [\lambda_2^{(\ell-1)} + \beta(f_s^{(\lambda_1^{(\ell)},\lambda_2^{(\ell-1)})} - \xi_s)]^+$ où $[.]^+ = \max(., 0)$
Critère d'arrêt	$\frac{1}{\beta}\lvert\lambda_1^{(\ell)} - \lambda_1^{(\ell-1)}\rvert \leq \epsilon_1$ $\frac{1}{\beta}\lvert\lambda_2^{(\ell)} - \lambda_2^{(\ell-1)}\rvert \leq \epsilon_2$

TABLE 4.1 – Solution numérique pour résoudre (4.22) pour un $\gamma \in [0, 1]$ fixé.

Puisque $I_{k-1}^{\mathcal{D}}$ et $I_{k-1}^{\mathcal{E}}$ dépendent de $C_1^{\mathcal{D}}, .., C_{k-1}^{\mathcal{D}}$ et $C_1^{\mathcal{E}}, .., C_{k-1}^{\mathcal{E}}$ respectivement, on peut écrire :

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,...,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}},C_1^{\mathcal{E}},..,C_{K-1}^{\mathcal{E}}} \sum_{k=1}^{K} \left\{ \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \right\} + \lambda_1 \cdot f_0 + \lambda_2 \cdot f_s \quad (4.27)$$

Pour la simplicité de notation, on va écrire$f_0(\rho_1, ..., \rho_K) = f_0$ et $f_s(\rho_1, ..., \rho_K) = f_s$.

Pour résoudre (4.22), on a utilisé l'algorithme itératif proposé dans la Table 4.1 pour mettre à jour λ_1 et λ_2 dans les simulations. Cet algorithme est basé sur la méthode du gradient pour mettre à jour alternativement λ_1 et λ_2.

Maintenant, on suppose que $\boldsymbol{\lambda_1}$ **et** $\boldsymbol{\lambda_2}$ **sont fixés** et on s'intéresse à résoudre (4.27). Tout d'abord, on observe que les états des décodeurs du récepteur légitime et de l'espion

dans un bloc k peuvent être écrits en fonction des états passés de la façon suivante :

$$I_k^{\mathcal{D}} = I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k \tag{4.28}$$

avec $I_0^{\mathcal{D}} = 0$, et

$$I_k^{\mathcal{E}} = I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k \tag{4.29}$$

avec $I_0^{\mathcal{E}} = \gamma$.

En utilisant (4.14) et (4.19), on peut exprimer (4.27) de la façon suivante :

$$\begin{aligned} J^{\lambda_1,\lambda_2} = \min_{\rho_1,\ldots,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},\ldots,C_{K-1}^{\mathcal{D}},C_1^{\mathcal{E}},\ldots,C_{K-1}^{\mathcal{E}}} \left\{ \sum_{k=1}^{K} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \right\} + \lambda_1 \cdot \left[\mathbb{E}_{C_1^{\mathcal{D}},\ldots,C_K^{\mathcal{D}}} \left\{ \mathbb{I}(I_K^{\mathcal{D}} < 1) \right\} \right] \\ + \lambda_2 \cdot \sum_{k=1}^{K-1} \left[\mathbb{E}_{C_1^{\mathcal{D}},\ldots,C_k^{\mathcal{D}}} \left\{ \mathbb{I}(I_{k-1}^{\mathcal{D}} < 1) - \mathbb{I}(I_k^{\mathcal{D}} < 1) \right\} \cdot \mathbb{E}_{C_1^{\mathcal{E}},\ldots,C_k^{\mathcal{E}}} \left\{ \mathbb{I}(I_k^{\mathcal{E}} > 1) \right\} \right] \\ + \lambda_2 \cdot \left[\mathbb{E}_{C_1^{\mathcal{D}},\ldots,C_{K-1}^{\mathcal{D}}} \left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \mathbb{E}_{C_1^{\mathcal{E}},\ldots,C_K^{\mathcal{E}}} \left\{ \mathbb{I}(I_K^{\mathcal{E}} > 1) \right\} \right] \end{aligned} \tag{4.30}$$

En utilisant (4.28), (4.29) et le fait que les canaux de l'espion et du récepteur légitime sont indépendants, le problème (4.30) peut être simplifié en le divisant en des sous problèmes d'optimisation plus simples à résoudre (voir annexe C) :

$$J^{\lambda_1,\lambda_2} = J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}})$$

$$\begin{aligned} J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}}) = \min_{\rho_1} \mathbb{E}_{C_1^{\mathcal{D}},C_1^{\mathcal{E}}} \Bigg\{ \rho_1 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_0^{\mathcal{D}} < 1) - \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1 < 1) \right\} \cdot \left\{ \mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1 > 1) \right\} \right] \\ + J_2^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1, I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1) \Bigg\} \end{aligned}$$

$$\begin{aligned} J_2^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}) = \min_{\rho_2} \mathbb{E}_{C_2^{\mathcal{D}},C_2^{\mathcal{E}}} \Bigg\{ \rho_2 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_1^{\mathcal{D}} < 1) - \mathbb{I}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2 < 1) \right\} \cdot \left\{ \mathbb{I}(I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 > 1) \right\} \right] \\ + J_3^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2, I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2) \Bigg\} \end{aligned}$$

...

$$J_K^{\lambda_1,\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} \mathbb{E}_{C_K^{\mathcal{D}}, C_K^{\mathcal{E}}} \left\{ \rho_K + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \left\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K > 1) \right\} \right] \right.$$
$$\left. + \lambda_1 \cdot \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1) \right.$$

D'une autre façon, $J_k^{\lambda_1,\lambda_2}$ $(k < K)$ et $J_K^{\lambda_1,\lambda_2}$ peuvent être aussi exprimés par :

$$J_K^{\lambda_1,\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} \ \rho_K + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_{K-1}^{\mathcal{E}}}{\rho_K} \right) \right\} \right] + \lambda_1 \cdot F_{C^{\mathcal{D}}} \left(\frac{1 - I_{K-1}^{\mathcal{D}}}{\rho_K} \right) \tag{4.31}$$

$$J_k^{\lambda_1,\lambda_2}(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) = \min_{\rho_k} \ \rho_k + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{D}}} \left(\frac{1 - I_{k-1}^{\mathcal{D}}}{\rho_k} \right) \right\} \cdot \left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_{k-1}^{\mathcal{E}}}{\rho_k} \right) \right\} \right]$$
$$+ \mathbb{E}_{C_k^{\mathcal{D}}, C_k^{\mathcal{E}}} \left\{ J_{k+1}^{\lambda_1,\lambda_2}(I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k, I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k) \right\} \tag{4.32}$$

où $F_{C^{\mathcal{D}}}$ et $F_{C^{\mathcal{E}}}$ sont les fonctions de densités cumulatives de $C^{\mathcal{D}}$ et $C^{\mathcal{E}}$ respectivement. On peut montrer que les fonctions de densité cumulative de $C^{\mathcal{D}}$ et $C^{\mathcal{E}}$ sont les suivantes,

$$F_{C^{\mathcal{D}}}(x) = 1 - e^{-\frac{2^{2x}-1}{\bar{h}}} \tag{4.33}$$

$$F_{C^{\mathcal{E}}}(x) = 1 - e^{-\frac{2^{2x}-1}{\bar{g}}} \tag{4.34}$$

en utilisant la définition de la fonction de densité cumulative et les distributions p_H et p_G données dans (4.3) et (4.4).

Par conséquence, la méthode de programmation dynamique est applicable pour faire l'optimisation puisque J^{λ_1,λ_2} est écrite sous forme d'une récursion de programmation dynamique.

Pour résoudre ce problème pour λ_1 et λ_2 fixés, on commence par la dernière équation $J_K^{\lambda_1,\lambda_2}$, afin d'obtenir la valeur de ρ_K qui minimise $J_K^{\lambda_1,\lambda_2}$ pour chaque couple de $I_{K-1}^{\mathcal{D}}$ et $I_{K-1}^{\mathcal{E}}$. Dans les simulations, on discrétise $I_{K-1}^{\mathcal{D}}$ et $I_{K-1}^{\mathcal{E}}$ en L_1 et L_2 points dans l'intervalle [0,1) et [γ,1] respectivement. Alors $\rho_K(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}})$ est une matrice de taille $L_1 \times L_2$. Le problème doit être résolu en commençant par l'étape K et en allant récursivement jusqu'à $k = 1$ pour trouver toutes les politiques optimales ρ_k (qui sont aussi des matrices de taille $L_1 \times L_2$, sauf pour $k = 1$ où ρ_1 contient un seul élément) pour des λ_1 et λ_2

donnés. Par conséquent, l'optimisation de la fonction $J^{\lambda_1\lambda_2}$ dans un espace de dimension très grande est réduite en $(K-1)\cdot L_1\cdot L_2+1$ problèmes d'optimisation unidimensionnels beaucoup plus simples à résoudre. Un exemple est donné dans l'annexe C pour illustrer la résolution de ce problème en utilisant la programmation dynamique lorsque $K=3$.

La résolution récursive du problème d'optimisation par la méthode du programmation dynamique, permet d'obtenir les politiques optimales d'adaptation du débit associées aux λ_1 et λ_2 fixés. Afin de mettre à jour λ_1 et λ_2, on a besoin de calculer les probabilités d'*outages* f_0 et f_s. Par conséquence, on doit calculer les distributions de probabilités jointes des $I_k^{\mathcal{D}}$ et $I_k^{\mathcal{E}}$ pour $k=1,..,K$ et les utiliser ensuite dans (4.14) et (4.19). En utilisant le fait que les canaux sont indépendants, la fonction de densité cumulative jointe de $I_1^{\mathcal{D}}, I_1^{\mathcal{E}}$, pour $k=1$, est :

$$F_{I_1^{\mathcal{D}}I_1^{\mathcal{E}}}(x,y)=\Pr\left(\rho_1\cdot C_1^{\mathcal{D}}<x,\gamma+\rho_1\cdot C_1^{\mathcal{E}}<y\right)=F_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right)\cdot F_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right)$$

En dérivant la fonction de densité cumulative par rapport à x et y, on obtient la densité de probabilité jointe :

$$p_{I_1^{\mathcal{D}}I_1^{\mathcal{E}}}(x,y)=\frac{1}{\rho_1}\cdot p_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right)\cdot\frac{1}{\rho_1}\cdot p_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right) \tag{4.35}$$

où $p_{C^{\mathcal{D}}}$ et $p_{C^{\mathcal{E}}}$ sont les densités des probabilités des variables aléatoires i.i.d $C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}$ et $C_1^{\mathcal{E}},..,C_K^{\mathcal{E}}$ respectivement. Les expressions de $p_{C^{\mathcal{D}}}$ et $p_{C^{\mathcal{E}}}$ sont obtenues en dérivant $F_{C^{\mathcal{D}}}(x)$ et $F_{C^{\mathcal{E}}}(x)$ par rapport à x :

$$p_{C^{\mathcal{D}}}(x)=2\cdot\log(2)\cdot p_H(2^{2x}-1)\cdot 2^{2x} \tag{4.36}$$

$$p_{C^{\mathcal{E}}}(x)=2\cdot\log(2)\cdot p_G(2^{2x}-1)\cdot 2^{2x} \tag{4.37}$$

Pour $k>1$, la fonction de densité cumulative jointe est calculée récursivement :

$$F_{I_k^{\mathcal{D}}I_k^{\mathcal{E}}}(x,y)=\Pr\left(I_{k-1}^{\mathcal{D}}+\rho_k\cdot C_k^{\mathcal{D}}<x,I_{k-1}^{\mathcal{E}}+\rho_k\cdot C_k^{\mathcal{E}}<y\right) \tag{4.38}$$

$$=\int_0^x\int_\gamma^y\Pr\left(I_{k-1}^{\mathcal{D}}+\rho_k\cdot C_k^{\mathcal{D}}<x,I_{k-1}^{\mathcal{E}}+\rho_k\cdot C_k^{\mathcal{E}}<y|I_{k-1}^{\mathcal{D}}=\alpha,I_{k-1}^{\mathcal{E}}=\beta\right)\cdot p_{I_{k-1}^{\mathcal{D}}I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\,d\alpha\,d\beta$$

$$= \int_0^x \int_\gamma^y F_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)}\right) \cdot F_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)}\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\ d\alpha\ d\beta$$

Alors la densité jointe, obtenue en dérivant la fonction de densité cumulative jointe, est obtenue récursivement en utilisant $p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x,y)$:

$$p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = \int_0^x \int_\gamma^y \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)}\right) \cdot \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)}\right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha,\beta)\ d\alpha\ d\beta \tag{4.39}$$

Dans le cas où $\rho_k(x,y) = 0$ on a $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y) = p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x,y)$ d'après (4.38).

En obtenant les valeurs optimales de λ_1 et λ_2, vérifiant les contraintes, on peut calculer le débit utile secret dans (4.15) en utilisant $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x,y)$ et $\rho_k(x,y)$. On rappelle que ce débit utile secret est obtenu pour un $\gamma \in [0,1]$ fixé. On discute maintenant le choix du γ. Dans les simulations, on a observé que le débit utile secret augmente lorsque γ augmente. Cependant, on a observé aussi que lorsque γ est plus grande qu'une certaine valeur entre 0 et 1, il est impossible de satisfaire les contraintes des probabilités d'*outages*. En d'autres termes, on ne peut pas obtenir des probabilités d'*outages* plus petites que les valeurs cibles fixées quelque soient les valeurs des multiplicateurs de Lagrange. Alors, on sera intéressé par la recherche de la valeur maximale de γ vérifiant les contraintes d'*outages*.

4.6 Application numérique

Comme application numérique, on a étudié l'exemple en fixant les paramètres suivants : $\overline{h} = 15$ dB, $\overline{g} = 5$ dB, $\xi_\epsilon = 10^{-3}$ et $\xi_s = 10^{-3}$. Les simulations ont été faite pour plusieurs valeurs du nombre maximal des transmissions K.

La Figure 4.6, montre le débit utile secret η en fonction du nombre maximal des transmissions K pour le schéma de la redondance incrémentale *"INR scheme"* décrit dans [48] (voir Fig.7 dans [48]) et le nouveau schéma adaptatif de la redondance incrémentale *"adaptive INR scheme"*. Les résultats montrent qu'un gain important en débit utile secret en utilisant le nouveau schéma. Cependant, lorsque K est petit ex. pour K=1 ou 3, le débit utile secret η reste négligeable en utilisant le nouveau schéma à cause d'une

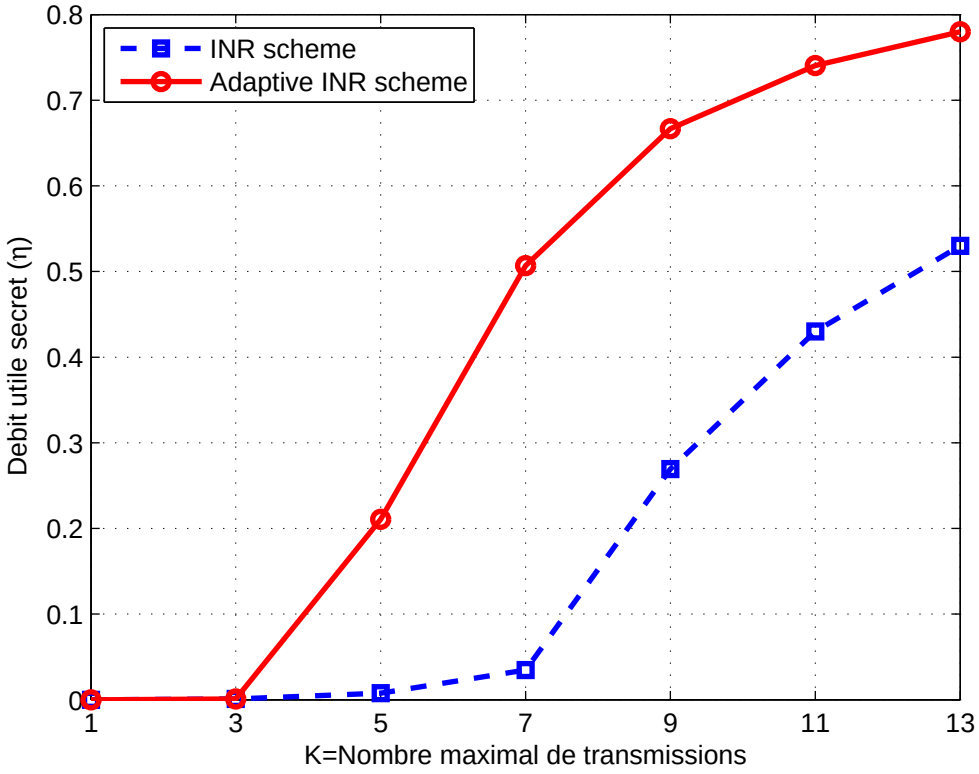

FIGURE 4.2 – Le débit utile secret η en fonction du maximum nombre de transmissions K.

diversité insuffisante. Le débit utile secret pour tous les schémas augmente pour $K > 3$.

Lorsque $K \to \infty$ le débit utile secret pour le schéma de la redondance incrémentale tend vers une valeur constante selon l'analyse asymptotique dans [48]. Cette valeur est égale à $0.5 \cdot \mathbb{E}\big[\log_2(1+h) - \log_2(1+g)\big] = 1.31$ en utilisant (4.3) et (4.4). On observe que lorsque $K = 13$, le schéma adaptatif atteint 60% de la limite maximale du débit utile secret alors que le schéma non-adaptatif atteint seulement 40%. Cela montre le gain important qu'on peut obtenir avec le schéma adaptatif de la redondance incrémentale.

4.7 Conclusion

Dans ce chapitre, on a considéré la communication fiable et sécurisée sur les canaux à écoute à évanouissement par blocs lorsque l'émetteur n'a pas d'information sur l'état instantané du canal. On a considéré les protocoles HARQ avec un nombre limité des tentatives de transmission et on a utilisé la programmation dynamique pour trouver la politique optimale d'adaptation du débit afin d'optimiser le débit utile secret pour la transmission avec des contraintes d'*outages*. On a montré que le schéma HARQ adaptatif avec redondance incrémentale proposé a un gain significatif en termes de débit utile en comparant au schéma non adaptatif avec redondance incrémentale.

Chapitre 5

Conclusions et perspectives

5.1 Conclusions

Dans ce travail de thèse, on a étudié des modèles de systèmes de diffusion avec des contraintes réalistes. On s'est concentré sur l'étude des canaux de diffusion Gaussiens avec une contrainte de puissance chez l'émetteur. Deux modèles de canaux de diffusion avec deux récepteurs ont été étudié : le premier est le canal de diffusion avec un message commun et un message destiné à un récepteur seulement, et le deuxième est le canal de diffusion avec message commun et un message confidentiel. Pour ces deux types de canaux, on a vu que les régions de capacité sont atteignables en utilisant des alphabets d'entrée Gaussiens. Cependant, ces alphabets ne sont pas réalisables en pratique. Dans les systèmes de transmission réels, les symboles transmis appartiennent à une constellation de taille finie (ex., M-PAM, M-QAM,..) ce qui rend les débits atteignables par les utilisateurs différents du cas de l'alphabet Gaussien.

Dans la première partie de cette thèse, on a étudié l'impact de la contrainte d'alphabet fini pour le canal de diffusion Gaussien avec deux utilisateurs dans deux cas : (1) lorsque l'émetteur a un message commun pour deux récepteurs et un message destiné à un récepteur seulement et (2) pour un canal de diffusion avec message commun et un message confidentiel. On a étudié les régions des débits atteignables pour plusieurs stratégies de transmission : le *time sharing*, la superposition de modulation et le codage

par superposition. Les régions des débits atteignables en utilisant la superposition de modulation et le codage par superposition ont été maximisées par rapport aux positions des symboles dans la constellation et par rapport à la distribution de probabilité jointe P_{UX}. Un algorithme a été proposé pour résoudre ce problème d'optimisation non-convexe pour les deux modèles de canaux de diffusion considérés. Les résultats ont montré que la contrainte d'alphabet fini peut changer des résultats bien connus dans le cas d'alphabet Gaussien. Précisément, on a vu que la superposition de modulation n'est pas la stratégie optimale dans le cas d'alphabet fini. En effet, le cas général du codage par superposition peut atteindre des gains importants en débits par rapport aux stratégies classiques (*time sharing* ou superposition de modulation). Pour le cas de superposition de modulation, la maximisation des débits atteignables apportent des gains plus importants lorsque la cardinalité de l'alphabet d'entrée augmente par rapport au cas où on maximise seulement les positions des symboles. Pour le cas du canal de diffusion avec message confidentiel, on a vu que le débit secret maximal n'est pas nécessairement atteignable lorsque la puissance totale disponible à l'entrée est utilisée pour transmettre le message secret. On a aussi discuté le compromis entre l'efficacité des stratégies de transmission et leur complexité d'implémentation. La comparaison entre les stratégies a été faite en termes de gains en débits atteignables et/ou en termes de gains sur le RSB. On a vu que dans certains cas, l'utilisation des schémas pratiques tels que le *time sharing* et la superposition de modulation résulte en des pertes très petits en débits atteignables par rapport au schéma optimal non-pratique. Par contre, dans d'autres cas, l'utilisation des stratégies complexes apportent des gains importants par rapport aux schémas classiques.

D'autre part, on a vu que les débits atteignables par les récepteurs dans un canal de diffusion Gaussien nécessitent la connaissance parfaite de l'état instantanée du canal par l'émetteur ce qui n'est pas souvent le cas dans les systèmes réels. Dans la dernière partie de cette thèse, on a considéré le canal à écoute à évanouissement par blocs lorsque l'émetteur n'a pas une information parfaite sur l'état instantané du canal mais connait seulement les statistiques. On a étudié un schéma adaptatif pour la communication sécurisée basée sur les protocoles HARQ en considérant des canaux de retour à niveaux

multiples du récepteur légitime et de l'espion vers l'émetteur. Par suite, le débit peut être adapté en utilisant les canaux de retour en permettant à la longueur des sous-mots de code pour changer à chaque retransmission. On a utilisé la programmation dynamique pour trouver la police optimale d'adaptation du débit afin de maximiser le débit utile secret pour la transmission sous des contraintes d'*outages*. On a montré que le schéma HARQ adaptatif avec redondance incrémentale proposé apporte un gain significatif en termes de débit utile secret en comparant au schéma non adaptatif pour un nombre maximal de transmission supérieur à un seuil déterminé.

5.2 Perspectives

Ce travail de thèse ouvre la voie à des diverses perspectives, extensions et généralisations. Tout d'abord, ce travail pourrait s'étendre à des constellations complexes à deux dimensions par exemple de type M-PSK ou M-QAM qui sont plus utilisées en pratique. Ainsi, l'impact de la contrainte d'alphabet fini sur les débits atteignables pour le canal de diffusion à deux utilisateurs pourrait être étudié dans le cas des constellations complexes. En plus, le calcul des débits atteignables avec contrainte d'alphabet fini a supposé un canal de diffusion Gaussien qui est un modèle de canal peu réaliste. Donc on pourrait imaginer comme extension de ce travail l'étude de l'impact de la contrainte d'alphabet fini pour les canaux de diffusion à évanouissement. La stratégie du mise en œuvre du *shaping* de la constellation en pratique pour générer des symboles non-équiprobables est aussi un défi pour les canaux de diffusion. Dans ce contexte, on trouve dans la littérature des travaux qui sont faits sur la mise en forme de la constellation pour les canaux point-à-point. On cite parmi eux la stratégie proposée par Le Goff et al. dans [81] pour la mise en forme du constellation PAM turbo-codée et avec entrelacement. Cette stratégie divise la constellation de "base" du signal transmis en deux ou plusieurs sous-constellations et utilise un *shaping code* pour choisir les signaux des sous-constellations de faible énergie plus fréquemment que les signaux des sous-constellations d'énergie plus grande.

De plus, dans le chapitre 4, on a étudié les protocoles HARQ pour un canal à écoute

en supposant que l'alphabet d'entrée est Gaussien. Ainsi, il est utile d'étendre cette analyse en prenant en considération la contrainte de l'alphabet fini. Dans ce contexte, une étude sur le débit utile secret des protocoles HARQ et sous contraintes de modulations est présentée dans [82]. La communication sécurisée avec une incertitude sur le canal est aussi une direction importante puisque l'incertitude sur le canal existe en pratique pour plusieurs raisons [83]. Par exemple, le *CSI* est d'habitude obtenu en envoyant des séquences d'apprentissage au niveau de l'émetteur et permettant au récepteur d'estimer le canal. L'estimation peut ne pas être parfaite, ce qui se traduit par des informations erronées ou inexactes au niveau du récepteur. Le *CSI* est fourni à l'émetteur via le canal à retour qui pourrait être limité et non fiable. Dans le chapitre 4 aussi, on a supposé qu'il existe des canaux de retour du récepteur légitime et de l'espion à la fois vers l'émetteur. Une extension de ce travail est actuellement en cours et consiste à étudier un cas plus réaliste dans lequel l'émetteur ne reçoit pas un retour de l'espion. De plus, on peut étudier le cas où le nombre additionnel de bits pour assurer la sécurité M_d est adapté à chaque transmission. Par suite, on aura plus de degrés de liberté et on espèrera plus de gains en débit utile secret.

Tout au long de ce travail, on a considéré un codage aléatoire et un décodage basé sur les séquences typiques. Un travail futur pourra considérer des schémas de codage et de décodage pratiques. Ainsi, il est intéressant de prendre en compte la présence d'un code correcteur d'erreurs dans la chaîne de transmission par exemple de type turbo ou LDPC. En ce qui concerne les codes secrets, des travaux existants sur la conception de ces codes incluent le codage *coset* [84], les codes LDPC [85] et les *nested codes* [86]. Un défi est la conception des codes secrets de débit compatible pour les canaux Gaussiens.

Annexe A

Article sur l'optimisation des débits atteignables pour les canaux de diffusion avec alphabet d'entrée fini ([1])

Achievable Rates Optimization For Broadcast Channels Using Finite Size Constellations Under Transmission Constraints

Z. Mheich and F. Alberge* and P. Duhamel

Univ. Paris-Sud, UMR8506 Orsay, F-91405; CNRS, Gif-sur-Yvette, F-91192;
Supelec, Gif-sur-Yvette, F-91192, 3 rue Joliot-Curie, 91192 Gif-sur-Yvette cedex, France
Tel: +33 1 69851757; fax: +33 1 69851765

Email: Z. Mheich - zeina.mheich@lss.supelec.fr; F. Alberge - alberge@lss.supelec.fr; P. Duhamel - pierre.duhamel@lss.supelec.fr;

*Corresponding author

Abstract

In this paper, maximal achievable rate regions are derived for power constrained AWGN broadcast channel involving finite constellations and two users. The achievable rate region is studied for various transmission strategies including superposition coding and compared to standard schemes such as time sharing. The maximal achievable rates are obtained by optimizing over both the joint distribution of probability and over the constellation symbol positions. A numerical solution is proposed for solving this non-convex optimization problem. Then, we consider several variations of the same problem by introducing various constraints on the optimization variables. The aim is to evaluate efficiency vs complexity tradeoffs of several transmission strategies, some of which (the simplest ones) can be found in actual standards. The improvement for each scheme is evaluated in terms of SNR savings for target achievable rates or/and percentage of gain in achievable rates for one user compared to a reference scheme. As an application, two scenarios of coverage areas and user alphabets are considered. This study allows to evaluate with practical criteria the performance improvement brought by more advanced schemes.

Keywords

AWGN broadcast channels, achievable rate region, hierarchical modulation, superposition modulation, superposition coding, constellation shaping, non-

convex optimization.

1 Introduction

During the past few decades, information networks have witnessed tremendous and rapid advances, based on the important growth in the adoption of new wireless technologies, applications and services, first from cellular networks and more recently for computer networks (WLANs). Consequently, wireless networks are exposed to capacity and coverage problems and the focus is now shifting towards capturing some of the aspects of realistic networks by studying natural network models such as models with broadcasting.

In 1972, achievable rate region is obtained by Cover in [1] for Gaussian broadcast channels with two outputs and generalized by Bergmans to broadcast channels with any number of outputs [2]. Roughly a year later, the optimality of the sets of achievable rates was established by Bergmans [3] and Gallager [4]. Superposition coding is a possible solution to achieve good rate regions in which information intended for high-noise receivers and information intended for low-noise receivers are superimposed and transmitted simultaneously on the same radio resource. The low-noise receivers can always decode messages intended for the high-noise receivers. Thus they effectively cancel out the interference due to the signal intended for the high-noise receivers, and then decode their own message. The high-noise receivers decodes its message by treating the low-noise receivers message as noise. Superposition coding appears in several contexts in information theory and is closely related to multilevel coding and unequal error protection [5], [6]. Cover showed [1] that superposition coding reaches the theoretical limit of the capacity region for two user Gaussian broadcast channel using an infinite Gaussian input alphabet for each user. A treatment of the case of multiple transmitter/receivers for the band-limited additive white Gaussian noise channel is given by Bergmans and Cover in [7] where it is proved that superposition coding can achieve higher rate region than orthogonal schemes such as frequency-division multiple access (FDMA) or time-division multiple access (TDMA). However, in actual transmissions systems, the channel input is constrained to a finite size alphabet with equal probability symbols. A well known practical implementation of superposition coding is hierarchical modulation, also called layered modulation, which uses constellations with non-uniformly spaced signal points creating different levels of error protection. Hierarchical modulation is used to mitigate the cliff effect in digital television broadcast and is included in various standards, such as Digital Video Broadcast for Terrestrial Television (DVB-T) [8], DVB to Handhelds (DVB-H) and DVB Satellite services to Handhelds (DVB-SH) [9] standard proposal for mobile digital TV transmission. A study about the performance of hierarchical modulation and a comparison with time sharing strategy in terms of achievable rates can be found in [10].

The restriction imposed by practical systems in using finite signaling constellation and equiprobable symbols reduces the achievable rates and leads to a

gap with the capacity region achieved with Gaussian input alphabets for AWGN broadcast channel. This gap can be reduced using a technique called constellation shaping. In fact, most results for constellation shaping with finite signal constellations consider only point to point communication systems [11]. Then the concept of constellation shaping has been adapted to most modern coding and modulation techniques as for example turbo-coding and BICM schemes [12]-[19]. For broadcast channels, the achievable rate region for two-user AWGN broadcast channels with finite input alphabets is derived in [20] when superposition of modulated signal is used as transmission strategy. In their work, the authors assume a uniform distribution over the finite input set. To our knowledge, no study is available about the maximization of the achievable rate region for two-user AWGN broadcast channels with finite size constellations by optimizing over both the joint probability distribution and constellation symbol positions for a broadcast transmission strategy. This general framework encompasses hierarchical modulations as a special case. In this paper, maximal achievable rate regions are derived for power constrained AWGN broadcast channel of two users with M-Pulse Amplitude Modulation (M-PAM) constellations of M points using various transmission strategies. A numerical solution is proposed for solving this non-concave optimization problem. In a typical broadcast system, there is a trade off between achievable rates and coverage areas. Therefore, we are interested in determining the transmission strategy which provides the best achievable rates or the maximal SNR gain for a given coverage scenario. The compromise between simplicity of implementation and expected gains is also evaluated.

The organization of the paper is as follows. Section 2 recalls some information theory results on broadcast channels and degraded broadcast channels. In section 3 various transmission strategies for broadcast systems are described. Section 4 gives a formulation of the problem in terms of optimization for the various transmission strategies under consideration. Then computational aspects are discussed. An iterative algorithm is proposed for the computation of maximal achievable rate regions using superposition coding (general case) and M-PAM constellation or in the particular case of superposition modulation. The proposed algorithm can handle an optimization with respect to the joint distribution of probability or with respect to the positions of constellation symbols. Both variables can also be considered jointly. Obviously, the best results are obtained for the most general case. Our target is to: *(i)* evaluate the loss experienced by using simple schemes, *(ii)* identify situations in which complex schemes (non-standard) lead to significant improvements. As an application, we consider, in section 5, several scenarios of coverage areas and user alphabets and we give conclusions about the transmission strategies which can provide the best trade off between efficiency and complexity of implementation.

2 AWGN Broadcast Channels

A two-receiver (users) broadcast channel (BC) consists of an input alphabet $\mathcal{X}$, two outputs alphabets $\mathcal{Y}_1$ (user 1), $\mathcal{Y}_2$ (user 2) and a conditional pdf $P_{Y_1Y_2|X}$ on $\mathcal{Y}_1 \times \mathcal{Y}_2$. Let X, Y_1 and Y_2 be random variables representing the input and outputs of the BC. Figure 1 depicts the two users BC with two independent messages W_1 and W_2. The encoder generates a codeword $x^n(w_1, w_2)$ of length n based on these two messages. Each user receives respectively y_1^n and y_2^n. A BC is said to be physically degraded if $P_{Y_1Y_2|X}(y_1, y_2|x) = P_{Y_1|X}(y_1|x) \cdot P_{Y_2|Y_1}(y_2|y_1)$ (i.e. $X \to Y_1 \to Y_2$ form a Markov chain). A BC is said to be stochastically degraded or degraded if there exists a random variable $\tilde{Y_1}$ which has the same conditional pdf as Y_1 given X such that $X \to \tilde{Y_1} \to Y_2$ form a Markov chain. We are interested in degraded BC because its capacity region is known, while it is not available for the general case.

In our system model, W_1 denotes the private message intended for receiver 1 only and W_2 is a common message for both receivers. A typical example of this situation is digital TV broadcasting to two different groups of receivers, classified according to their channel conditions, where the basic signal (common signal) should be available to all receivers. The higher quality is realized by adding the basic signal with an incremental signal (private signal for receivers of good channel conditions) which carries TV signal with a high data rate, such as HDTV.

Let R_1 and R_2 be the rates at which the transmitter is sending W_1 and W_2 respectively. Thus user 1 achieves $R_1 + R_2$ while user 2 achieves R_2. The capacity region of the degraded broadcast channel $X \to Y_1 \to Y_2$ in figure 1 is the convex hull of the closure of rate pairs $(R_1 + R_2, R_2)$ satisfying:

$$R_1 \leq I(X; Y_1|U) \tag{1}$$

$$R_2 \leq I(U; Y_2) \tag{2}$$

for some joint distribution $P_{UXY_1Y_2} = P_{UX} \cdot P_{Y_1|X} \cdot P_{Y_2|X}$ on $\{\mathcal{U} \times \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2\}$ [21]. $P_{Y_1|X}$ and $P_{Y_2|X}$ are conditional pdfs that depend on the channel model. P_{UX} is the joint probability distribution of U and X, where the auxiliary random variable U has cardinality bounded by $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$. The capacity region is achieved using superposition coding where U serves as the center of a cloud of codewords that can be distinguished by both receivers. Since the capacity region of a BC depends only on the conditional marginals, the capacity region of the stochastically degraded BC is equal to that of the corresponding physically degraded channel. Cover [1] showed that in the case of binary symmetric BC and AWGN BC, superposition coding expands the rate region beyond that achievable with time sharing.

Now consider the Gaussian broadcast channel with two users. Without loss of generality, assume that Y_1 is less noisy than Y_2. It can easily be shown that scalar Gaussian broadcast channels are equivalent to a degraded channel,

$$Y_1 = X + Z_1 \tag{3}$$

$$Y_2 = X + Z_2 = Y_1 + Z_2' \tag{4}$$

where $Z_1 \sim \mathcal{N}(0, \sigma_1^2)$, $Z_2 \sim \mathcal{N}(0, \sigma_2^2)$, $Z_2' \sim \mathcal{N}(0, \sigma_2^2 - \sigma_1^2)$ and Z_1, Z_2' are independent. Thus Gaussian BC is stochastically degraded. We assume an average power constraint on the transmitted power P defined as $\mathbb{E}[X^2] \leq P$. The received signal to noise ratio for each user is $SNR_i = \frac{P}{\sigma_i^2}$, where $SNR_1 > SNR_2$ and σ_i^2 is the variance of the noise Z_i. The capacity region of the AWGN-BC is the set of rate pairs $(R_1 + R_2, R_2)$ such that:

$$R_1 \leq C(\alpha \cdot SNR_1) \tag{5}$$

$$R_2 \leq C(\frac{(1-\alpha) \cdot SNR_2}{\alpha \cdot SNR_2 + 1}) \tag{6}$$

for all $\alpha \in [0, 1]$, where $C(x) = \frac{1}{2} \cdot \log_2(1 + x)$. The theoretical limit of two-user AWGN BC is achieved by using signal superposition [1].

3 Broadcast transmission strategies

In this section, various transmission strategies for broadcast systems are described. The strategies are presented in ascending order of implementation complexity. Specifically, by moving from one strategy to another, we release some constraints on the system implementation to reach finally the most complex strategy that can be used to broadcast information for users. Obviously, since the simple schemes can be understood as adding constraints to the most general case, their are less efficient in terms of attainable rates.

3.1 Time Sharing (TS)

Time sharing has been widely used in broadcast systems as broadcast transmission strategy. In time sharing scheme, a percentage of time is used to send one message and the rest of the time is used to send another message. Thus it is practical to implement because the rate pairs can be achieved by strategies used for point to point channel and sharing the time between messages. As in previous works on broadcasting, this situation serves as a reference for the more advanced schemes. In this work, a time sharing scheme with standard constellation M-PAM (Fig.2) is considered when symbols are used with equal probability. A standard M-PAM constellation is defined as a constellation with M real symbols belonging to $\mathcal{X} = \{M - 1 - 2 \cdot (i-1), \text{for } i = 1, ..., M\}$. During the time slot dedicated to send a message, only one data stream is sent using the entire set of constellation points. In classical implementations of time sharing, the conventional M-PAM symbols are equally spaced and used with equal probability.

3.2 Hierarchical Modulation (HM)

In two layers hierarchical modulation, constellation symbols are used to transmit two data streams simultaneously for two users [22][23]. Constellation symbols

are usually chosen with the same probability but may be non-equally spaced. These symbols can be considered as the sum of two lower order modulations, one for each user. The modulation with higher power is used for the "bad" channel, the one with smallest power for the "good" channel. Hence, the encoding using hierarchical modulation can be separable for the two streams which is more practical.

This is explained here using 4-PAM as an example. Fig.3 shows the constellation diagram of a hierarchical 4-PAM with parameter $\ell = \ell_1/\ell_2$ used to determine the spacing between the groups of constellation points (clouds). ℓ is the ratio of the spacing between the groups to the spacing between individual points within a group. Standard values of ℓ are 1, 2 and 4. When ℓ increases, with a fixed total transmission power P, the two points from both sides of origin form a cloud. The location of a point within its cloud is regarded as the information for the "good" user. The other information, i.e. the number of the cloud in which the point is located is the information for the "bad" user. In this way, two separate data streams can be made available for transmission. Formally, we are still dealing with 4-PAM but, in the hierarchical interpretation, it is viewed as the combination of 2 BPSK modulations which have different robustness to noise. In other words, the service coverage areas differ in size for both users. The better-protected data stream is referred to as the High- Priority (HP) stream which is mapped in Fig.3 to the most significant bit. The other one, is referred to as the Low-Priority (LP) stream (Fig.3) and mapped in Fig.3 to the least significant bit. Receivers with good reception conditions can receive both streams, while those with poorer reception conditions may only receive the high priority stream considering the LP stream as noise. This corresponds to a specific labeling of the modulation.

3.3 Superposition Modulation (SM)

In superposition modulation [24], the M constellation points are used such that the labeling is separable, *i.e.* $M = M_1 M_2$, and that the M points are obtained by adding (in $\mathbb{R}$) two rv's X_1 and X_2, of cardinality M_1 and M_2 respectively ($M_1, M_2 \in \mathbb{N} \setminus \{0, 1\}$). Thus this scheme is with an enlarged set of feasible labelings than in the previous case [25],[26]. This leads also to $U \equiv X_2$ for superposition modulation because user 2 can distinguish only U.

This work studies several cases of superposition modulation. First, when the constellation symbols for each user are used with equal probability. This case will be denoted as $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$. This is a practical case since the encoding of the messages is separable and symbols are used with equal probability as in real transmission systems. Then, the constraint of using equiprobable symbols is released, the symbols of user constellations can be dependent and used with non-equal probability (P_{UX} non-uniform). Thus the encoding here is done jointly for the two messages. This strategy will be denoted $SM_{\overline{\mathcal{X}},P_{UX},P_X}$ when the symbols take the values of a standard M-PAM and $SM_{\mathcal{X},P_{UX},P_X}$ otherwise. In the latter case, the symbol positions can take arbitrary values and will be considered as variables to be optimized. The definition of superposition mod-

ulation can be generalized using more general form for P_{UX} than the uniform case. In superposition modulation, 2^{nR_2} independent codewords $u^n = x^{(2)n}(w_2)$ of length n are generated according to P_U and for each of these codewords, 2^{nR_1} satellite codewords $v^n = x^{(1)n}(w_1)$ are generated and added to form codewords $x^n(w_1, w_2) = u^n + v^n$ according to $P_{X|U}$. Thus, the fine information v^n is superimposed on the coarse information u^n.

Note that the capacity region of Gaussian broadcast channel is achieved using this coding scheme and successive cancellation decoding where U ($\equiv X_2$) and V ($\equiv X_1$) are independent random variables following normal distributions. However, we do not assume here that U and V are independent. Consequently, for superposition modulation, P_{UX} takes a specific expression. As an example, consider an 8-PAM modulation. In that case, the transmitted signal at time k is the sum of the two users signals and is given by $x_k = x_k^{(1)} + x_k^{(2)}$ where $x_k^{(1)} \in \mathcal{X}_1$ and $x_k^{(2)} \in \mathcal{X}_2$ with $M_1 \cdot M_2 = 8$. Two configurations are possible either $M_2 = 4$ ($\mathcal{X}_1$ is a BPSK and $\mathcal{X}_2$ is a 4-PAM) or $M_2 = 2$ ($\mathcal{X}_1$ is a 4-PAM and $\mathcal{X}_2$ is a BPSK). In both cases, P_{UX} is a sparse matrix of size $M_2 \times M$ with expression

$$P_{UX} = \begin{bmatrix} p_{00} & p_{01} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p_{12} & p_{13} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_{24} & p_{25} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_{36} & p_{37} \end{bmatrix} \quad if\ M_1 = 2, M_2 = 4 \tag{7}$$

$$P_{UX} = \begin{bmatrix} p_{00} & p_{01} & p_{02} & p_{03} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_{14} & p_{15} & p_{16} & p_{17} \end{bmatrix} \quad if\ M_1 = 4, M_2 = 2 \tag{8}$$

where $P_{UX}[i, j] = p_{i-1,j-1} = \Pr\{U = u_{i-1}, X = x_{j-1}\}$. In both cases, the number of elements to be computed is 8.

Note also that P_{UX} and $\mathcal{X}$ (of cardinality M) determine the labeling of the input signal constellation for a fixed labeling for $\mathcal{X}_1$ and $\mathcal{X}_2$ [25],[26]. Thus the information can be distinguished using the labeling. Consider for example a label l_k^u of $log_2(|\mathcal{X}_2|)$ binary labels for u_k and l_j^v of $log_2(|\mathcal{X}_1|)$ binary labels for v_j with $k \in \{0, .., |\mathcal{X}_2| - 1\}$ and $j \in \{0, .., |\mathcal{X}_1| - 1\}$. Obviously, the M symbols $x_i,\ i \in \{0, .., |\mathcal{X}| - 1\}$ carry $log_2(M)$ binary labels which are the concatenations of the labels of u_k and v_j such as $x_i = u_k + v_j$.

Part of this work on superposition modulation was presented in [25],[26],[27], where the achievable rate regions for $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ and $SM_{\mathcal{X},P_{UX},P_X}$ strategies are analyzed using a 4-PAM constellation in [25],[26] and for {4,8,16}-PAM constellations in [27]. In this work, the achievable rates are also derived for $SM_{\overline{\mathcal{X}},P_{UX},P_X}$ using {4,8,16}-PAM constellations.

3.4 Superposition Coding (SC)

Superposition coding is one of the basics of coding schemes in network information theory. This idea was first introduced by Cover in an information theoretic study of broadcast channels [1].

In superposition coding, the joint distribution of probability P_{UX} can take a more general form than in the case of superposition modulation. In this case the labeling cannot allow to distinguish between the common information and the private information for user 1, a fact which increases the decoder complexity. Indeed, since the auxiliary random variable U has cardinality bounded by $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$, we use the name general superposition coding or superposition coding simply to describe the case where $|\mathcal{U}| = \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$. For superposition coding and with M-PAM modulation, P_{UX} is an $M \times M$ matrix with elements $p_{i,j}$.

The basics of superposition coding are briefly recalled below; a detailed description is given in [28]. In this scheme, 2^{nR_2} sequences $u^n(w_2)$,$w_2 \in [1, 2^{nR_2}]$ each i.i.d.,are generated randomly and independently to represent the coarse message each according to $\prod_{i=1}^{n} p_U(u_i)$. For each auxiliary sequence $u^n(w_2)$, randomly and conditionally independently generate 2^{nR_1} sequences $x^n(w_1, w_2)$,$w_1 \in [1, 2^{nR_1}]$, each according to $\prod_{i=1}^{n} p_{X|U}(x_i|u_i(w_2))$ to represent the fine message w_1. Thus in superposition coding, the auxiliary random variable U serves as a cloud center for the information, distinguishable by both receivers. In this case, the decoding of information by users is based on large block joint typicality. This comes in contrast with the simpler cases where the message for user 2 was carried by the center of *modulation* clouds which imply a possible scalar detection.

The achievable rates for superposition coding will be studied for various strategies corresponding to different constraints on P_{UX} and/or $\mathcal{X}$.

An exhaustive list of all the strategies under consideration is given in table 1 where redundant configurations are omitted.

4 Achievable Rate Regions

For a two user Gaussian BC, the theoretical limit of the capacity region is achieved using Gaussian input alphabet for each user. However, practical implementation constraints impose the use of finite input alphabets, and the symbols are usually chosen with equal probability. These restrictions contribute to increase the gap between the capacity region achieved with infinite Gaussian inputs and the throughput obtained in practical situations. In this section, we are interested in computing the achievable rate region of power constrained AWGN BC when the transmitted signal is modulated using an M-PAM constellation, under the various situations described above. Since the last case (superposition coding) encompasses all previous ones as special cases, the corresponding optimization problems can be solved with the same strategy, which is detailed in this section.

4.1 Problem Formulation

Consider a two users memoryless AWGN broadcast channel ($SNR_1 > SNR_2$) with signal power constraint P. The channel input belongs to a finite set

Transmission	Variables	Constraints	Designation
SM	$\mathcal{X}$	Uniform distribution for P_{UX}	$SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$
SM	P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$	Symbol locations: M-PAM	$SM_{\overline{\mathcal{X}},P_{UX},P_X}$
SM	$\mathcal{X}$ P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$		$SM_{\mathcal{X},P_{UX},P_X}$
SC	P_{UX} s.t. $\sum_i p_{i,j} = \frac{1}{M}$	Symbol locations: M-PAM Uniform distribution for P_X	$SC_{\overline{\mathcal{X}},P_{UX},\overline{P_X}}$
SC	$\mathcal{X}$ P_{UX} s.t. $\sum_i p_{i,j} = \frac{1}{M}$	Uniform distribution for P_X	$SC_{\mathcal{X},P_{UX},\overline{P_X}}$
SC	P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$	Symbol locations: M-PAM	$SC_{\overline{\mathcal{X}},P_{UX},P_X}$
SC	$\mathcal{X}$ P_{UX} s.t. $\sum_{i,j} p_{i,j} = 1$		$SC_{\mathcal{X},P_{UX},P_X}$

Table 1: Strategies under consideration

$\mathcal{X} = \{x_0, ..., x_{M-1}\} \subset \mathbb{R}$ represented by an M-PAM constellation. Assume a symmetric input signal constellation with respect to the origin. Since $\mathcal{U}$ has cardinality bounded by $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$ and the output alphabet cardinality for an AWGN channel is infinite, we have $|\mathcal{U}| \leq |\mathcal{X}|$. Thus $|\mathcal{U}| \leq M$.

To determine the maximal achievable rate region using superposition coding, consider the case $|\mathcal{U}| = M$. For superposition modulation, we take into account the specificity on P_{UX} given in section 3.3. We also consider within the same framework the problem of maximizing the achievable rates under additional constraints on optimization variables (P_{UX} and $\mathcal{X}$): standard M-PAM symbols values, uniform distribution for P_{UX}, uniform distribution for P_X. The problem of maximizing the achievable rates under a specific situation is solved subject to a combination of constraints according to table 1. We recall that in this work, message w_2 is a common message to both receivers and w_1 is a private message to user 1. Thus the achievable rate region (R_2 vs. $R_1 + R_2$) can be obtained by solving the weighted sum rate ($\theta \cdot R_1 + (1-\theta) \cdot R_2$) maximization for $\theta \in [0, 0.5]$. Indeed, for $\theta = 0$, we maximize the common information rate R_2 and when $\theta = 0.5$ we maximize the rate achieved by user 1 ($R_1 + R_2$). Using (1) and (2), the optimization problem under consideration is:

$$\begin{array}{ll} \max_{P_{UX},\mathcal{X}} & \theta \cdot I(X;Y_1|U) + (1-\theta) \cdot I(U;Y_2) \\ s.t. & p_{ij} \geq 0 \quad \forall i,j \\ & \sum_{i,j} p_{ij} \cdot x_j^2 \leq P \end{array} \tag{9}$$

and subject to the constraint on the joint pdf P_{UX} or on $\mathcal{X}$ given in table 1 for each strategy, where $p_{ij} = \Pr\{U = u_i, X = x_i\}$, $j \in \{0, .., M-1\}$ and $i \in \{0, .., |\mathcal{U}| - 1\}$. The two mutual information $I(X;Y_1|U)$ and $I(U;Y_2)$ can be

written as follows

$$I(X;Y_1|U) = \sum_{i,j} \int_{-\infty}^{+\infty} p_{ij} P_{Y_1|X}(y_1|x_j) \log \frac{(\sum_{j'} p_{ij'}) P_{Y_1|X}(y_1|x_j)}{\sum_{j'} p_{ij'} P_{Y_1|X}(y_1|x_{j'})} dy_1 \quad (10)$$

$$I(U;Y_2) = \sum_{i} \int_{-\infty}^{+\infty} (\sum_{j} p_{ij} P_{Y_2|X}(y_2|x_j)) \log \frac{\sum_{j'} p_{ij'} P_{Y_2|X}(y_2|x_{j'})}{(\sum_{j'} p_{ij'})(\sum_{i',j'} p_{i'j'} P_{Y_2|X}(y_2|x_{j'}))} dy_2 \quad (11)$$

where all logarithms are taken base 2. The AWGN channel for each user is characterized by the conditional pdf

$$P_{Y_i|X}(y|x) = \frac{1}{\sqrt{2\pi\sigma_i^2}} . e^{-\frac{(y-x)^2}{2\sigma_i^2}} \quad i \in \{1,2\} \quad (12)$$

When $\theta = 0$ or $\theta = 1$ and for $|\mathcal{U}| = M$ (which are referred in this paper as point-to-point (PtP) channel case), the individual achievable rates R_2 and R_1 are maximized respectively. The problem (9) is equivalent to

$$\begin{array}{ll} \max_{P_X, \mathcal{X}} & I(X;Y_k) \\ s.t. & p_i \geq 0 \quad \forall i \\ & \sum_i p_i = 1 \\ & \sum_i p_i \cdot x_i^2 \leq P \end{array} \quad (13)$$

where $p_i = \Pr\{X = x_i\}$, $i \in \{0, .., M-1\}$ is the input probability distribution and $k \in \{1,2\}$. When $\theta = 0$ or 1, problem (13) is solved for $k = 2$ and 1 respectively with $I(X;Y_k)$ given by

$$I(X;Y_k) = \int_{-\infty}^{+\infty} \sum_{j} p_j P_{Y_k|X}(y_k|x_j) \log \frac{P_{Y_k|X}(y_k|x_j)}{\sum_{j'} p_{j'} P_{Y_k|X}(y_k|x_{j'})} dy_k \quad (14)$$

For the time sharing scheme using standard constellation, the achievable rate pair $(R_1 + R_2, R_2)$ is such that [1]:

$$\begin{cases} R_1 = \alpha \overline{R_1} \\ R_2 = (1-\alpha) \overline{R_2} \end{cases} \quad (15)$$

where $\overline{R_1}$ and $\overline{R_2}$ are achievable rates for PtP channel using standard M-PAM constellation at SNR_1 and SNR_2 respectively. Varying α from 0 to 1 yields achievable rate region.

Problem (9) is not convex, therefore direct numerical optimization is inefficient. Clearly, an exhaustive search is not feasible as the complexity would be exponential in the total number of variables. An iterative method for solving (9) is proposed in the next section.

4.2 Numerical solution

Consider a regularized version of (9) as:

$$L(P_{UX}, x_0, .., x_{M-1}, s) = \theta \cdot I(X;Y_1|U) + (1-\theta) \cdot I(U;Y_2) + s \cdot (P - \sum_{i=0}^{|\mathcal{U}|-1} \sum_{j=0}^{M-1} p_{ij} \cdot x_j^2) \tag{16}$$

where s is a regularization parameter. For a given value of s, the optimization problem in (16) is solved (for the most general case) with respect to P_{UX} and to $\mathcal{X} = (x_0, x_1, ..., x_{M-1})$ alternately until convergence:

$$P_{UX}^{(\ell)} = \arg \max_{P_{UX} \in \mathcal{C}} L(P_{UX}, x_0^{(\ell-1)}, .., x_{M-1}^{(\ell-1)}, s) \tag{17}$$

$$\mathcal{X}^{(\ell)} = \arg \max_{\mathcal{X}} L(P_{UX}^{(\ell)}, x_0, .., x_{M-1}, s) \tag{18}$$

where ℓ is the iteration index and $\mathcal{C}$ denotes the set of constraints on P_{UX} and can be defined either as $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$ or as $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_i p_{i,j} = \frac{1}{M}\}$ (equiprobable symbols). The optimization problem in (17) with constraint set $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$ can be handled by a modified Blahut-Arimoto type algorithm [29]. Indeed, in order to take into account the regularization, we can show that the "Blahut Arimoto "-type algorithm proposed in [30] for broadcast channels should be modified by replacing equation (19) of lemma 3 in [30] by $q^*(u,x) = \frac{\beta[Q,\tilde{Q},\bar{Q}](u,x) \cdot e^{-s\frac{x^2}{1-\theta}}}{\sum_{u',x'} \beta[Q,\tilde{Q},\bar{Q}](u',x') \cdot e^{-s\frac{x'^2}{1-\theta}}}$ instead of $q^*(u,x) = \frac{\beta[Q,\tilde{Q},\bar{Q}](u,x)}{\sum_{u',x'} \beta[Q,\tilde{Q},\bar{Q}](u',x')}$ where $\beta[Q,\tilde{Q},\bar{Q}](u,x)$ is defined in equation (19) of [30]. When there is an additional constraint on constellation symbols to be equiprobable *i.e.* $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1 \text{ and } \sum_i p_{i,j} = \frac{1}{M}\}$, the "Blahut Arimoto "-type algorithm in [30] should also be modified to take into account the additional constraint. In this case, equation (19) of lemma 3 in reference [30] should be replaced by $q^*(u,x) = \frac{1}{|\mathcal{X}|} \cdot \frac{\beta[Q,\tilde{Q},\bar{Q}](u,x)}{\sum_u \beta[Q,\tilde{Q},\bar{Q}](u,x)}$, which does not depend on s, where $\beta[Q,\tilde{Q},\bar{Q}](u,x)$ is defined in equation (19) in this reference.

Now consider (18). The function $L(P_{UX}^{(\ell)}, x_0, .., x_{M-1}, s)$ is not a concave function for all $\mathcal{X} \in \mathbb{R}^M$. However, we observed in our experiments that $L(P_{UX}^{(\ell)}, x_0, .., x_{M-1}, s)$ is a concave function if $\mathcal{X} \in \mathcal{D}$ where $\mathcal{D} = \{\mathcal{X} \in \mathbb{R}^M : |x_i - x_j| > d \ \ \forall i,j \in \{0, .., M-1\}$ and $i \neq j\}$ and d depends on the size of the constellation and on the *SNR*. Since we are interested in finding non degenerated constellation, we restrict the optimization process to $\mathcal{D}$. Then a simplex method is used to perform the optimization with initial value in $\mathcal{D}$.

The alternative maximization method can at least increase the objective function in each iteration. In the experiments, we have observed that this method converges at least to a local maximum (denoted $p_{i,j}^*(s)$, $x_j^*(s)$, $0 \leq j \leq M-1$, $0 \leq i \leq |\mathcal{U}| - 1$).

Step 0	$s \leftarrow s^{(0)}$	
Step k	Step 0	$\mathcal{X} \leftarrow \mathcal{X}^{(0)}$ where $\mathcal{X} = (x_0, x_1, .., x_{M-1})$
	Step ℓ	$P_{UX}^{(\ell)} = \arg\max_{P_{UX} \in \mathcal{C}} L(P_{UX}, \mathcal{X}^{(\ell-1)}, s^{(k-1)})$ $(P1)$ $\mathcal{X}^{(\ell)} = \arg\max_{\mathcal{X}} L(P_{UX}^{(\ell)}, \mathcal{X}, s^{(k-1)})$ $(P2)$
	Stopping criterion	$\lvert L(P_{UX}^{(\ell)}, \mathcal{X}^{(\ell)}, s^{(k)}) - L(P_{UX}^{(\ell-1)}, \mathcal{X}^{(\ell-1)}, s^{(k-1)}) \rvert \leq \epsilon_L$
	$s^{(k)} = [s^{(k-1)} - \beta(P - \sum_{i,j} p_{ij}^*(s^{(k-1)}) \cdot (x_j^*(s^{(k-1)}))^2)]^+$ where $[.]^+ = \max(., 0)$	
Stopping criterion	$\lvert s^{(k)} - s^{(k-1)} \rvert \leq \epsilon_s$	

Table 2: Numerical solution for solving (9)

We discuss now the choice of s. Since we do not know a priori which value of s may correspond to the satisfaction of the equality power-constraint, we propose to use an iterative process as follows:

$$s^{(k+1)} = \left[s^{(k)} - \gamma \cdot \left(P - \sum_{i=0}^{|\mathcal{U}|-1} \sum_{j=0}^{M-1} p_{ij}^*(s^{(k)}) \cdot (x_j^*(s^{(k)}))^2 \right) \right]^+ \tag{19}$$

where $[.]^+$ is defined as $[.]^+ = \max(., 0)$. The value of s is increased or decreased with the sign of $P - \sum_{i=0}^{|\mathcal{U}|-1} \sum_{j=0}^{M-1} p_{ij}^*(s^{(k)}) \cdot (x_j^*(s^{(k)}))^2$. The process stops when the power constraint is fulfilled. The proposed algorithm is summarized in table 2. Obviously, when constellation symbols are constrained to the values of a standard constellation, (P2) which is defined in table 2 will not be used. Similarly, when P_{UX} is uniform, (P1) is not used. An alternative interpretation of this algorithm is to recognize that $L(P_{UX}, x_0, .., x_{M-1}, s)$ is the Lagrangian dual of problem 9. Eq. (17-18) is an iterative method for solving

$$f(s) = \max_{P_{UX}, x_0, .., x_{M-1}} L(P_{UX}, x_0, .., x_{M-1}, s) \tag{20}$$

The dual optimization problem $\min_{s.t.\ s \geq 0} f(s)$ is solved in (19) with a gradient-type algorithm. Since $f(s)$ is convex [31], a gradient-search method is guaranteed to converge to a global optimum.

5 Result analysis

5.1 Point to point channel

We present in this section, the results of maximizing achievable rates for PtP case using M-PAM constellations with M=4, 8, 16 and for different values of *SNR*. To evaluate the contribution of constellation shaping, we compare, for a fixed *SNR*, the maximal achievable rate calculated by the algorithm proposed in

the previous section to the "standard constellation" rate, whose symbols are used with equal probability, at the same SNR in terms of SNR saving (called SNR shaping gain). The SNR shaping gain depicted in Fig. (4) is the gain obtained with a fully optimized constellation ($P_{\mathcal{X}}$ and $\mathcal{X}$) compared to the standard M-PAM constellation and when symbols are used with the same probability. To avoid the complexity of constructing nearly optimal input distribution codes, another method for doing constellation shaping is to optimize only the position of symbols in the constellation. Each signal point is assumed to be chosen with the same probability however the position of each point in the constellation is optimized. The corresponding shaping gain is given in Fig. (5). We observe the following. The shaping gain depends on the SNR and on the size of the constellation. The maximum gain is obtained for mid-range SNR. The distribution of probability $P_{\mathcal{X}}$ (not reported) is very similar to the sampling of a gaussian distribution. With the half-optimized constellation ($\mathcal{X}$ only), a significant degradation is observed for mid range SNR compared to the fully optimized constellation. Hence, we can conclude that symbol pdf optimization is useless at low and high SNR whereas the fully-optimized constellation is efficient for mid-range SNR, in which case the gain increases with the size of the constellation.

5.2 Broadcast channel

Current broadcast systems are using two practical transmission schemes for sending information to users: orthogonal schemes in which the time and/or frequency is split between the users and superposition modulation schemes where the constellation for each user is fixed. In this section, a comparison is provided between these standard schemes and various (more complex) transmission strategies such as superposition coding. The effect of constellation shaping is evaluated by analyzing the achievable rate region curves obtained for an M-PAM constellation (M=4, 8, 16) and for several pairs (SNR_1, SNR_2). The following schemes are considered:

- Time Sharing using standard M-PAM (TS).
- Superposition Modulation (SM) - 3 possible configurations (see table 1)
- Superposition coding (SC) - 4 possible configurations (see table 1)

In the following, we denote by the "case 1" of superposition modulation when $M_1 = 2, M_2 = 4$ and when $M_1 = 2, M_2 = 8$. The "case 2" is when $M_1 = 4, M_2 = 2$ and when $M_1 = 4, M_2 = 4$. The "case 3" refers to the case when $M_1 = 8, M_2 = 2$.

Achievable rate region curves are provided in Fig. 6-11 for $M = 4, 8, 16$. For each value of M, the display of the results is limited to two different pairs of SNR. In complement with the achievable rate region curves, comparisons are also conducted in terms of SNR savings for target achievable rates (Maximum Shaping Gain) and in terms of Maximum Percentage of Gain for user 1. These

two quantities are defined below.

Definition 1 *Consider two transmission strategies (A and B). The pair of rates* $(R_1 + R_2, R_2)$ *is achieved for* (SNR_1, SNR_2) *with A and for* $(SNR_1 + \Delta SNR, SNR_2 + \Delta SNR)$ *with B. The shaping gain (with A compared to B) is* ΔSNR*. The maximum shaping gain is defined as:*

$$MG_{SNR_{dB}}(A|B) = max_{R_2} \Delta SNR \tag{21}$$

Definition 2 *Consider two transmission strategies (A and B). For a given pair of SNR* (SNR_1, SNR_2) *and a fixed value of* R_2*, the achievable pair of rates is* $(R_1^A + R_2, R_2)$ *resp.* $(R_1^B + R_2, R_2)$ *with A resp. B. The gain on the achievable rate for user* 1 *is given by*

$$G_{R_1}(A|B) = \frac{(R_1^A + R_2) - (R_1^B + R_2)}{R_1^B + R_2} \cdot 100 \ (\%) \tag{22}$$

The maximum gain on the achievable rate for user 1 *(with A compared to B) is given by*

$$MG_{R_1}(A|B) = max_{R_2} G_{R_1}(A, B) \tag{23}$$

5.2.1 Superposition modulation

In this section, the three possible configurations of Superposition Modulation are compared. We can see from Fig. 6 to 11 that $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ (optimization of $\mathcal{X}$ only) outperforms $SM_{\overline{\mathcal{X}},P_{UX},P_X}$ (optimization of P_{UX} only) in terms of maximal achievable rates per user when $M = 4$. For $M = 8$ and 16, $SM_{\overline{\mathcal{X}},P_{UX},P_X}$ can achieve slightly higher rates than $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$. The implementation of a system with constellation symbols with non-standard positions and generated with the same probability is less complex than the implementation of a system which generates symbols with non-uniform joint distribution of probability. Thus, $SM_{\overline{\mathcal{X}},P_{UX},P_X}$ does not seem to be of interest since it is not very efficient in terms of achievable rates and is more complex to implement.

Figures of achievable rate region show that an improvement can be obtained with $SM_{\mathcal{X},P_{UX},P_X}$ (full optimization) compared to $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ (optimization of $\mathcal{X}$ only) and depending on $\delta_{SNR} = SNR_1 - SNR_2$. Numerical values of the maximum gain in achievable rate (MG_{R_1}) and of the maximum *SNR* savings ($MG_{SNR_{dB}}$) are given in table 3. We observe the following. A slight gain in terms of achievable rates can be translated into a noticeable gain in terms of *SNR* saving. The maximum shaping gain increases with the constellation size. Thus, constellation shaping for SM strategy seems more useful for high values of M. The analysis of the optimal matrix P_{UX} (results not reported) leads to the conclusion that X_1 and X_2 are not independent in general when using finite-size constellations. We observe also that the maximum shaping gain for $SM_{\mathcal{X},P_{UX},P_X}$ versus $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ increases when δ_{SNR} decreases, independently of M. In particular full optimization (vs optimization of the symbol position) does not provide significant improvement for large *SNR* gap in SM strategy.

M	SNR_1	SNR_2	$MG_{SNR_{dB}}(A\|B)$	$MG_{R_1}(A\|B)$
4	10	8	0.39	7.46%
		6	0.17	3.51%
		4	0.05	1.77%
		2	0.01	0.38%
8	16	14	$0.71^{(M_1=4,M_2=2)}$	$20.17\%^{(M_1=4,M_2=2)}$
		12	$0.57^{(M_1=4,M_2=2)}$	$13.21\%^{(M_1=4,M_2=2)}$
		10	$0.41^{(M_1=4,M_2=2)}$	$13.07\%^{(M_1=2,M_2=4)}$
		8	$0.33^{(M_1=2,M_2=4)}$	$18.93\%^{(M_1=2,M_2=4)}$
16	18	16	$1.05^{(M_1=8,M_2=2)}$	$10.67\%^{(M_1=8,M_2=2)}$
		14	$0.87^{(M_1=8,M_2=2)}$	$11.54\%^{(M_1=8,M_2=2)}$
		12	$0.64^{(M_1=8,M_2=2)}$	$12.08\%^{(M_1=4,M_2=4)}$
		10	$0.49^{(M_1=8,M_2=2)}$	$19.53\%^{(M_1=4,M_2=4)}$

Table 3: Comparison of $SM_{\mathcal{X},P_{UX},P_X}$ (A) and $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$) (B) with respect to $MG_{SNR_{dB}}$ and MG_{R_1}

5.2.2 Time-Sharing (TS) or Superposition Modulation (SM)?

This section compares two strategies (TS and SM) classically considered in broadcast systems. In Fig. 6 and 7 ($M = 4$), we observe that the achievable rate region can be split into 2 parts. Indeed, for small and large values of R_2, TS is better than SM. On the contrary, SM is better than TS for middle-range values of R_2. Under a given rate requirement for one user, we can thus determine the best transmission strategy. We can also observe that the region in which SM is better than TS becomes small for larger values of SNR_2. With $M = 8$ (Fig. 8 and 9), the area in which SM is better than TS increases (compared to $M = 4$) by considering the union of the two possible configurations for SM: $M_1 = 2$, $M_2 = 4$ (case 1) and $M_1 = 4$, $M_2 = 2$ (case 2). This is particularly true when δ_{SNR} increases. We also observe that TS can achieve higher rates than SM (case 1) for good SNR_2 values. Indeed, the maximum rate of user 2 with SM is the maximum individual rate for a 4-PAM constellation whereas it is the individual user rate achieved using standard 8-PAM in the TS case. For low SNR_2 values, optimized 4-PAM may achieve higher rate than standard 8-PAM thus SM becomes better in this interval. For a 16-PAM constellation (Fig. 10 and 11), SM is always better than TS for the studied pairs of (SNR_1, SNR_2). Table 4 shows the maximum percentage of improvement in achievable rate of user 1 by TS when using $SM_{\mathcal{X},P_{UX},P_X}$ (full optimization) strategy in the interval where $SM_{\mathcal{X},P_{UX},P_X}$ is better than TS. Clearly, the maximum percentage of improvement increases when δ_{SNR} increases and an important gain is obtained for high values of δ_{SNR} as in the case of $SNR_1 = \delta_{SNR} = 10dB$ for a 4-PAM where the percentage of gain on achievable rate of user 1 varies between 0 and 40.7%. For a 8-PAM constellation, the percentage of gain on achievable rate of user 1 varies between 0 and 30.21% when $SNR_1 = 16\ dB$ and $\delta_{SNR} = 8$

dB. For a 16-PAM, percentages of improvements can be up to 35.08% when $SNR_1 = 18dB$ and $\delta_{SNR} = 8dB$. We can conclude that SM is a better option than TS especially for large δ_{SNR} values. TS is optimal in the region where we want to maximize the rate of user 2 for good values of SNR_2 because the single user rate achieved by TS is the rate achieved using standard M-PAM constellation (the constellation is split between users with SM). Thus, SM seems more gainful than TS when we want to serve users with very diverse SNRs.

5.2.3 Is Superposition Coding necessary?

For the three constellations under consideration ($M = 4, 8, 16$), the maximal achievable rate region obtained by the optimal general case of superposition coding when we consider the general form of P_{UX} (SC) can achieve, depending on M and user SNRs, a large region of rate pairs ($R_1 + R_2$, R_2) that cannot be achieved neither by TS nor by SM. Even when we fully optimize SM ($SM_{\mathcal{X},P_{UX},P_X}$) we are far from maximal achievable rate region. Sometimes the maximal achievable rate region curve is very close or even coincides with the $SM_{\mathcal{X},P_{UX},P_X}$ achievable rate region in a pair of rates ($R_1^* + R_2^*$, R_2^*). This is the case when $SM_{\mathcal{X},P_{UX},P_X}$ is the optimal superposition coding in terms of achievable rates. We can see for example in Fig. 6 that the pair of rates ($R_1^* + R_2^* = 1.096$, $R_2^* = 0.531$ which corresponds to the optimal rate pair when we optimize the general case of SC for $\theta = 0.23$) is an intersection point with $SM_{\mathcal{X},P_{UX},P_X}$ achievable rate region.

We are interested now in the numerical evaluation of the gain in rate of user 1 ($R_1 + R_2$) when we use $SC_{\mathcal{X},P_{UX},P_X}$ (full optimization) compared to the best strategy between TS and SM. This gain ($MG_{R_1}(SC_{\mathcal{X},P_{UX},P_X}|TS \bigcup SM_{\mathcal{X},P_{UX},P_X})$ calculated in % is the distance between the limit of the maximal achievable rate region and the limit of the union of achievable rate regions of TS and $SM_{\mathcal{X},P_{UX},P_X}$. The results are reported in table 4. We observe that the part of the maximal achievable rate region which is unachievable by TS and SM, is bigger when M is small because we observe that for the case of 4-PAM we have one configuration for SM. However, we have two configurations of SM for 8-PAM constellation and three configurations for 16-PAM constellation. Thus when M increases, the union of achievable rates for all SM cases tends to the sets of achievable rates by the general superposition coding. Asymptotically, we know that when $M \to \infty$, $SM_{\mathcal{X},P_{UX},P_X}$ is the optimal superposition coding scheme because it allows to achieve the capacity region for two-user AWGN BC using Gaussian alphabet for each user. Thus the maximum gain in user 1 rate decreases when constellation order M increases. We observe also that the gain in achievable rates is high for high values of δ_{SNR}. On the other hand, the experiments show that by using the general superposition coding strategy with the constraint that symbols should be equiprobable ($SC_{\mathcal{X},P_{UX},\overline{P_X}}$), the loss is limited compared to the full optimization ($SC_{\mathcal{X},P_{UX},P_X}$), 4.84%, 7.66% and 3.94% for the simulated pairs of (SNR_1, SNR_2) when $M = 4$, 8 and 16 respectively. This means that we can use equiprobable symbols with, in general, a small loss in achievable rates. However, $SC_{\mathcal{X},P_{UX},\overline{P_X}}$ is not an interesting

M	SNR_1	SNR_2	$MG_{R_1}(A\|B)$	$MG_{R_1}(A\|C)$
4	10	8	6.13%	6.72%
		6	11.14%	11.65%
		4	18.50%	16.69%
		2	28.43%	18.9%
		0	40.70%	23.54%
8	16	14	$7.80\%^{(M_1=2,M_2=4)}$	7.89%
		12	$13.60\%^{(M_1=2,M_2=4)}$	11.43%
		10	$21.15\%^{(M_1=2,M_2=4)}$	14.96%
		8	$30.21\%^{(M_1=2,M_2=4)}$	14.71%
16	18	16	$10.36\%^{(M_1=2,M_2=8)}$	2.96%
		14	$16.42\%^{(M_1=4,M_2=4)}$	2.94%
		12	$24.68\%^{(M_1=4,M_2=4)}$	5.29%
		10	$35.08\%^{(M_1=4,M_2=4)}$	4.80%

Table 4: Comparison of $SM_{\mathcal{X},P_{UX},P_X}$ (A)vs TS (B). Comparison of $SC_{\mathcal{X},P_{UX},P_X}$ (A) vs $TS \bigcup SM_{\mathcal{X},P_{UX},P_X}$ (C).

case when $SM_{\mathcal{X},P_{UX},P_X}$ can achieve better rates since SM is less complex to implement than SC.

Moreover, with standard M-PAM symbols the two possible configurations ($SC_{\overline{\mathcal{X}},P_{UX},P_X}$ (optimization of P_{UX} and P_X) and $SC_{\overline{\mathcal{X}},P_{UX},\overline{P_X}}$ (optimization of P_{UX} only)) gives very similar results in most considered pairs of SNR. We also observe that the loss in maximum achievable rate experienced by user 1 with $SC_{\overline{\mathcal{X}},P_{UX},P_X}$ is less than 10% under the rate experienced with $SC_{\mathcal{X},P_{UX},P_X}$. Thus we can use standard values of symbol positions without loosing much on achievable rates.

In general one can conclude that fixing constellations of users (i.e. assigning labels to the constellation so that we distinguish between the bits intended for each user) is not optimal for coding and may result in important loss in terms of rates for systems using finite-size constellations especially for low-order constellations. A better solution is to determine the optimal alphabet of the auxiliary alphabet U which is not necessarily a constellation and then to generate the codewords x^n which are not necessarily the sum of two codewords (see paragraph 3.4).

6 Application : coverage extension

We first consider a transmission over a broadcast channel with finite size input alphabet. For simplicity of the illustration and without loss of generality, let us assume that the existing user alphabet belongs initially to a standard constellation whose symbols are used with equal probability. We assume that existing user is at distance d_0 from the sender achieving a rate R_0. Some information is

also to be transmitted to an upgraded layer of users. The sender can use up to 16 symbols, then several transmission schemes can be used. We are interested in comparing the transmission schemes to serve the new user under two scenarios: either the new user is closer to the transmitter than the existing user or the new user is farther than the existing one. For a target rate R_0 that is fixed for the existing user and achievable using a standard M-PAM and equiprobable symbols, we are interested in determining the variation of the coverage's diameter ratio between the two layer of users as a function of the achievable rate by the upgraded user for various broadcast transmission strategies. We assume that $SNR \propto \frac{1}{d^2}$.

6.1 The sender can use up to 16 symbols

6.1.1 Scenario 1

In this scenario, the system consists initially of one layer of users. Now assume that the data information is also to be transmitted to a second layer of users with higher SNR. In the following, we keep the notation from the preceding section where the user with greater SNR is denoted by user 1. Thus, in this scenario the legacy receivers are denoted by user 2 which is at a distance d_2 from the transmitter and achieving a rate R_0 when the data is modulated using standard 4-PAM constellation and equiprobable symbols. The upgraded receivers are denoted by user 1 ($SNR_1 > SNR_2$). We intend that the good user receives more throughput than user 2 via the use of 16-PAM.

In this example SNR_2 is fixed to 10 dB. Initially, user 2's alphabet belongs to a 4-PAM standard constellation (see section 3.1) and the rate transmitted to user 2 is $R_0 = 1.582$ bits/ch. use.

Now, a new layer of users called user 1 is introduced in the system with $SNR_1 > SNR_2$. Our target is to provide the maximum bit rate to the new user without changing R_0 or d_0 and using a 16-PAM. By enlarging the constellation and optimizing the symbol positions and probability distribution, we ensure that the rate of the initial user will not decrease after introducing a new user.

Consider now the results for the following strategies which can achieve a positive private-message rate for user 1: time sharing using standard 16-PAM, $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}} M_2 = 8/M_1 = 2$ (optimization of $\mathcal{X}$ only), $SM_{\mathcal{X},P_{UX},P_X} M_2 = 8/M_1 = 2$ (full optimization) and $SC_{\mathcal{X},P_{UX},P_X}$ (full optimization). Fig.12 illustrates the variation of d_1/d_2, which is the ratio of the diameter of the coverage area for user 1 over the diameter of the initial coverage area for user 2, as a function of the achievable rate for user 1 for a target rate $R_0 = 1.582$ for user 2.

Let assume for example that the new user is midway between the transmitter and user 2 ($d_1/d_2 = 0.5$). Fig.12 shows that the most simple case of superposition modulation ($SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}} M_2 = 8/M_1 = 2$) provides 16.3% more bit rate than time sharing for the new user. If we move immediately to a more complex case and optimize P_{UX} ($SM_{\mathcal{X},P_{UX},P_X} M_2 = 8/M_1 = 2$), a gain of 21% is obtained on the bit rate of user 1 comparing to time sharing. This gain on achievable rate for the new user is equivalent to a gain of $1dB$ on SNR_1 com-

paring to superposition modulation with uniform P_{UX}. However if we move to the most general case of superposition coding, it doesn't provide significant gain comparing to superposition modulation.

Now we assume that the new user is close to the transmitter such that $d_1/d_2 = 0.2$. We observe that the gain on the bit rate of user 1 using the simple case of superposition modulation increases to 45.7% comparing to time sharing. By moving to a more complex case ($SM_{\mathcal{X},P_{UX},P_X} M_2 = 8/M_1 = 2$), a gain of 47.8% is obtained on the bit rate of user 1 comparing to time sharing. We observe also that it is relevant in this case to move to the most general case of superposition coding since it provides a gain of 61.8% on the bit rate of user 1 comparing to time sharing.

Consequently, using superposition modulation provides always noticeable gain comparing to time sharing. The general case of superposition coding $SC_{\mathcal{X},P_{UX},P_X}$ is useful when user 1 is close to the transmitter but not when it is close to user 2.

6.1.2 Scenario 2

Initially, consider a system of one layer of users, denoted by user 1, at a distance d_1 from the transmitter and achieving a rate R_0. Moreover, the alphabet of user 1 belongs to a standard 8-PAM constellation. In this example, SNR_1 is fixed to 18 dB. Thus user 1 can achieve a rate $R_0 = 2.73$ $bits/ch.\ use$ in the initial situation. In this scenario, we want to serve a second layer of users denoted by user 2 which is farther to the transmitter than the existing user i.e. $SNR_2 < SNR_1$.

Achievable rates for user 2 are obtained at different distance d_2 from the transmitter and using various transmission strategies for a target rate of user 1 equal to R_0 and a coverage diameter for user 1 fixed to d_1. Fig.13 illustrates the variation of d_2/d_1, which is the ratio of the diameter of the coverage area for user 2 over the diameter of the initial coverage area for user 1, as a function of the achievable rate for user 2 when a target rate for user 1 is fixed to $R_0 = 2.73$ $bits/ch.\ use$.

We observe in Fig.13 that superposition modulation can always achieve better rates for user 2 than time sharing using 16-PAM. Let assume first that we want to increase the diameter of the coverage area for the new user (user 2) such that $d_2/d_1 = 4$. Time sharing provides a bit rate less than 0.06 $bits/ch.use$. The most simple case of superposition modulation ($SM_{\mathcal{X},P_{UX},P_X} M_2 = 2/M_1 = 8$) provides a significant improvement on the achievable rate for user 2 which is equal to 0.4 $bits/ch.use$ in this case. If we increase the complexity by optimizing the joint probability distribution P_{UX}, we obtain 35% more bit rate for user 2 comparing to superposition modulation with uniform P_{UX}. If we move to the general case of superposition coding, we gain only 10% on the bit rate of the new user comparing to superposition modulation (see table 5). However when the new layer of users is at distance $d_2 = 2.25\ d_1$, the general case of superposition coding provides a significant gain of 41% on the achievable rate of user 2 comparing to superposition modulation.

d_2/d_1	SNR_2	MG_{R_2}	M_2/M_1	d_2/d_1	SNR_2	MG_{R_2}	M_2/M_1
1.2589	16	4.9416	8/2	3.1623	8	16.7443	2/8
1.4125	15	20.1521	4/4	3.5481	7	12.6033	2/8
1.5849	14	12.7522	4/4	3.9811	6	10.5427	2/8
1.7783	13	8.2192	4/4	4.4668	5	10.3343	2/8
1.9953	12	7.4536	4/4	5.0119	4	11.7414	2/8
2.2387	11	41.4993	2/8	5.6234	3	16.0961	2/8
2.5119	10	30.8293	2/8	6.3096	2	22.8535	2/8
2.8184	9	22.9121	2/8	7.0795	1	32.6194	2/8

Table 5: Comparison of $SC_{\mathcal{X},P_{UX},P_X}$ and $SM_{\mathcal{X},P_{UX},P_X}$ M_2-PAM/M_1-PAM w.r.t the gain in achievable rate of user 2: MG_{R_2} (%), where SNR_1=18 dB

Consequently, the general case of superposition coding can bring significant gains comparing to superposition modulation depending on the diameter of coverage area for the new layer of users. For superposition modulation, optimizing the joint distribution of probability P_{UX} provides often significant shaping gains.

6.2 The cardinality of the existing user alphabet is kept fixed :

In this section, we study the scenarios 1 (and 2) supposing that the legacy receivers will continue working as in the initial situation, still using 4-PAM (8-PAM). The system consists initially to one layer of users at distance d_0 from the transmitter and achieving a rate R_0. Now we want to change the transmitter such that upgraded receivers closer (farther) in range will be able to decode a refinement (coarse) layer and using a 16-PAM constellation. Thus only time sharing with $M_1 = M_2 = 4$ ($M_1 = 8$, $M_2 = 2$) and superposition modulation strategies can be used. We aim to study how small the reduction in legacy coverage can be made depending on the rate of the refinement (coarse) information achieved by the upgraded users. Thus suppose that the legacy coverage can be reduced from d_0 to d_2 (from d_0 to d_1). We have studied this problem for $SNR_0 = 12$ dB and for $SNR_1 - SNR_2 = 4$ dB in scenario 1 (and for $SNR_0 = 16$ dB, $SNR_2 = 14$ dB in scenario 2). Figures 14 (and 15) represent the reduction in coverage d_2/d_0 (and d_1/d_0 respectively) as a function of the rate of the refinement R_1 (of the coarse R_2), while the rate achieved by the legacy receivers is kept fixed to its initial situation, *i.e.* R_0.

We observe in figures 14 (and 15) that the gain of superposition modulation strategies over time sharing becomes more important when d_2/d_0 (d_1/d_0) is small. These figures show that using superposition modulation when both symbol positions and P_{UX} are optimized, we gain around 5 % from the initial coverage comparing to the case of superposition modulation where symbols are used with equal probability. We can observe also that a reduction of only 10% and 20% in coverage area for the existing user can serve the upgraded user with a rate up to 20% and 35% (9% and 15%) from the rate achieved by the legacy

users, using $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$. Consequently, by using $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$, the legacy receivers still use 4-PAM (8-PAM in scenario 2) and we can serve a new layer of users with an acceptable rate, a small reduction in coverage area and with less complexity comparing to $SM_{\mathcal{X},P_{UX},P_X}$.

7 Conclusion

In this work we considered the problem of maximizing the achievable rate region for power constrained AWGN broadcast channel of two users using M-PAM constellations. The achievable rate region are given for various transmission strategies. Maximal achievable rate region for superposition coding and superposition modulation are obtained using constellation shaping. An iterative algorithm was proposed to solve this optimization problem. Then the efficiency of several strategies are compared. For superposition modulation, results showed that constellation shaping seems more useful for high values of M. Moreover, the gain in using a complex case of superposition modulation increases when the SNR gap between users decreases. We observed also that superposition modulation outperforms time sharing in a large part of the achievable rate region. On the other hand, it is shown that using the general case of superposition coding can bring important gains comparing to classical schemes. We observed also that in the case of finite input alphabet, superposition modulation is not the optimal strategy as in the case of Gaussian input alphabets. Finally, in order to make clear that this paper provides useful tools for the system designer, we considered two scenarios of coverage areas and user alphabets where the systems served initially one layer of users. Then we propose to serve a second layer of users and we evaluate the achievable rate of the new layer depending on the broadcast strategy. To improve the system performance compared to time sharing, we can optimize the joint probability distribution and symbol positions of the superimposed modulations or consider the general case of superposition coding. In this work we showed that the optimization of probabilities was often useful but not always. However, superposition coding brings sometimes significant gains comparing to superposition modulation depending on the diameter of coverage area for the new layer of users.

This work can also be extended to two dimensional constellations like M-QAM and other channel models. The maximization achievable rates using various transmission strategies can be performed also using the proposed algorithm based on alternative maximization with respect to symbol positions and the joint distribution of probability.

References

1. Cover TM: **Broadcast Channels**. *IEEE Trans.on Inform.Theory* 1972, **18**:2–14.
2. Bergmans PP: **Random Coding Theorem for Broadcast Channels With Degraded Components**. *IEEE Trans. on Inform. Theory* 1973, **19**(2).
3. Bergmans PP: **A Simple Converse for Broadcast Channels with Additive White Gaussian Noise**. *IEEE Trans. on Inform. Theory* 1974, **20**:279–280.
4. Gallager RG: **Capacity and Coding for Degraded Broadcast Channels**. *Probl. Infor. Transm.* 1974, :185–193.
5. Imai G, Hirakawa S: **A New Multilevel Coding Method Using Error Correcting Codes**. *IEEE Trans. on Inform. Theory* 1977, **23**:371–377.
6. Ungerboeck G: **Channel Coding with Multilevel/Phase Signals**. *IEEE Trans. on Inform. Theory* 1982, **28**:55–67.
7. Bergmans PP, Cover TM: **Cooperative Broadcasting**. *IEEE Trans. on Inform. Theory* 1974, **20**:317–324.
8. **European Telecommunications Standards Institute, Digital Video Broadcasting (DVB), Framing Structure, Channel Coding and Modulation for Digital Terrestrial Television, ETSI EN 300 744**.
9. **European Telecommunications Standards Institute, "Digital Video Broadcasting (DVB), System Specifications for Satellite Services to Handheld Devices (SH) Below 3 GHz" ETSI TS 102 585**.
10. Meric H, Lacan J, Amiot-Bazile C, Arnal F, Boucheret ML: **Generic Approach for Hierarchical Modulation Performance Analysis: Application to DVB-SH**. In *Wireless Telecommunications Symposium*, New York, USA 2011.
11. Calderbank AR, Ozarow LH: **Nonequiprobable Signaling on the Gaussian Channel**. *IEEE Trans. on Inform. Theory* 1990, **36**(4):726–740.
12. Sommer D, Fettweis G: **Shaping by Non-Uniform QAM for AWGN Channels and Applications Using Turbo Coding**. In *ITG Conference Source and Channel Coding* 2000:81–86.
13. Fragouli C, Wesel RD, Sommer D, Fettweis GP: **Turbo Codes with Non-Uniform Constellations**. In *Proc. IEEE Int. Conf. Communications* 2001.
14. N Varnica XM, Kavcic A: **Capacity of Power Constrained Memoryless AWGN Channels with Fixed Input Constellations**. In *GLOBECOM, Volume 2* 2002:1339–1343.
15. Raphaeli D, Gurevitz A: **Constellation Shaping for Pragmatic Turbo-Coded Modulation With High Spectral Efficiency**. *IEEE Trans. on Commun.* 2004, **52**(3):341–345.
16. LeGoff SY, Khoo BK, Tsimenidis CC, Sharif BS: **Constellation Shaping for Bandwidth-Efficient Turbo-Coded Modulation With Iterative Receiver**. *IEEE Transactions on Wireless Communications* 2007, **6**(6):2223–2233.
17. Ngo NH, Barbulescu SA, Pietrobon SS: **Performance of Nonuniform M-ary QAM Constellation on Nonlinear Channels**. In *Australian Communications Theory Workshop*, Australia 2005.
18. Zhang J, Chen D, Wang Y: **A New Constellation Shaping Method and Its Performance Evaluation in BICM-ID**. In *Vehicular Technology Conference Fall (VTC 2009-Fall)* 2009.

19. Valenti M, Xiang X: **Constellation Shaping for Bit-Interleaved LDPC Coded APSK**. *IEEE Transactions on Communications* 2012, **60**(10):2960–2970.

20. Huppert C, Bossert M: **On Achievable Rates in the Two User AWGN Broadcast Channel with Finite Input Alphabets**. In *ISIT*, Nice, France 2007.

21. Cover TM, Thomas JA: *Elements of Information Theory*. Wiley, Second Edition 2006.

22. Gledhill J, Macavock P, Miles R: **DVB-T: Hierarchical Modulation**. *DVB* 2000.

23. Schertz A, Weck C: **Hierarchical Modulation-The Transmission of Two Independent DVB-T multiplexes on a single frequency**. *EBU Techn.* 2003.

24. Singh V: **On Superposition Coding for Wireless Broadcast Channels**. *Master's thesis*, Royal Institute of Technology, Sweden 2005, `[www.ee.kth.se/php/modules/publications/reports/2005/IR-SB-EX-0507.pdf]`.

25. Mheich Z, Duhamel P, Szczecinski L, Alberi-Morel ML: **Constellation Shaping for Broadcast Channels in Practical Situations**. In *Proc. of the 19th European Signal Processing Conference*, Barcelona, Spain 2011.

26. Mheich Z, Alberi-Morel ML, Duhamel P: **Optimization of Unicast Services Transmission for Broadcast Channels in Practical Situations**. *Bell Labs Technical Journal* 2012, **17**:5–24.

27. Mheich Z, Alberge F, Duhamel P: **On the Efficiency of Transmission Strategies for Broadcast Channels Using Finite Size Constellations**. In *Proc. of the 21st European Signal Processing Conference*, Marrakech 2013.

28. Cover TM: **Comments on Broadcast Channels**. *IEEE Trans. on Inform. Theory* 1998, **44**(6).

29. Blahut RE: **Computation of Channel Capacity and Rate-Distortion Functions**. *IEEE Trans. on Inform. Theory* 1972, **18**(4).

30. Yasui K, Matsushima T: **Toward Computing the Capacity Region of Degraded Broadcast Channel**. In *ISIT* 2010.

31. Bertsekas DP: *Nonlinear Programming*. Athena Scientific, second edition edition 1999.

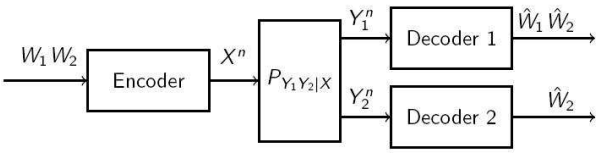

Figure 1: The two-user broadcast channel

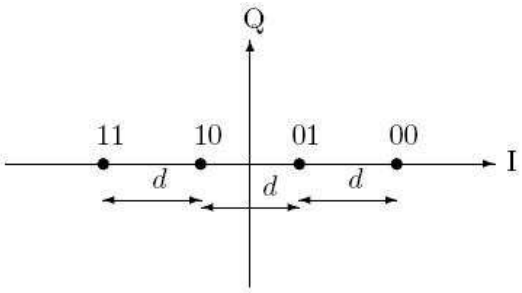

Figure 2: 4-PAM with equally spaced symbols

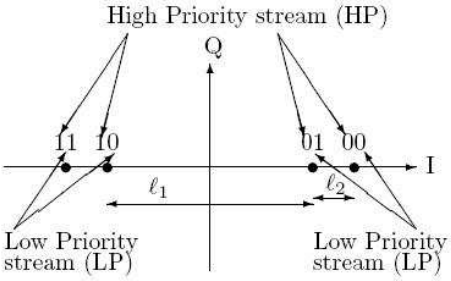

Figure 3: Hierarchical 4-PAM with parameter $\ell = \ell_1/\ell_2$

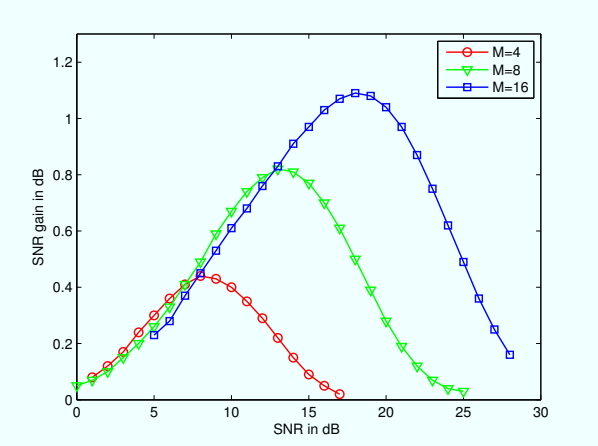

Figure 4: *SNR* shaping gain in dB vs PtP channel *SNR* - Optimal $\mathcal{X}$ and $P_{\mathcal{X}}$ vs Standard Constellation

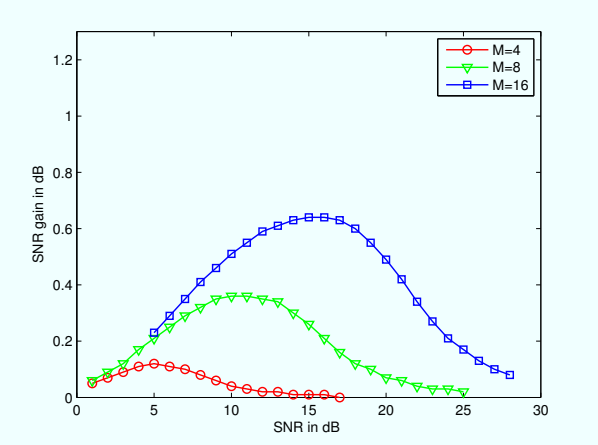

Figure 5: *SNR* shaping gain in dB vs PtP channel *SNR* - Optimal $\mathcal{X}$ vs Standard Constellation

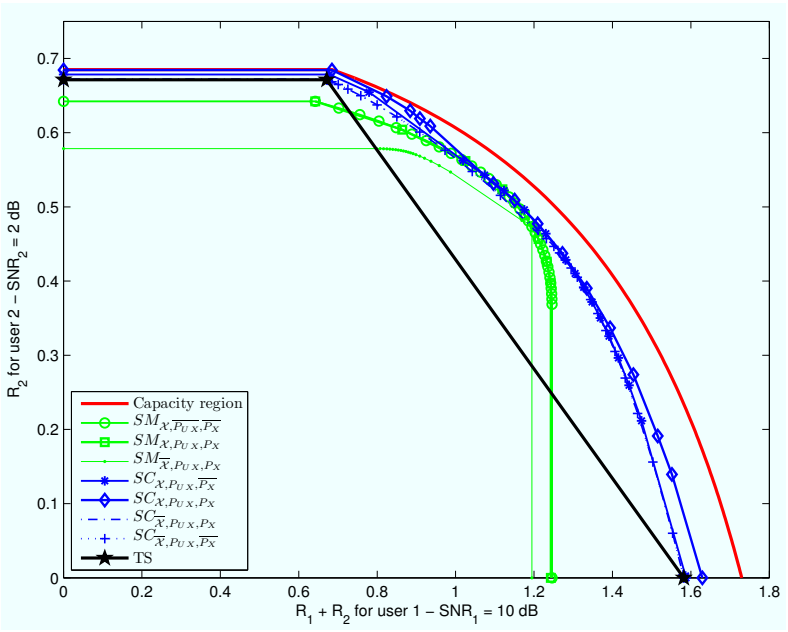

Figure 6: Achievable rate regions with $M = 4$ and $(SNR_1, SNR_2) = (10dB, 2dB)$

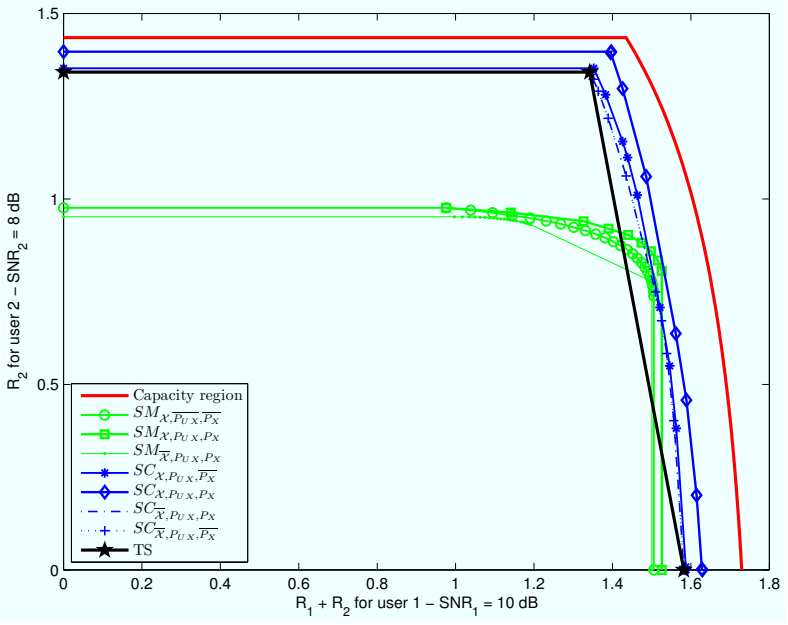

Figure 7: Achievable rate regions with $M = 4$ and $(SNR_1, SNR_2) = (10dB, 8dB)$

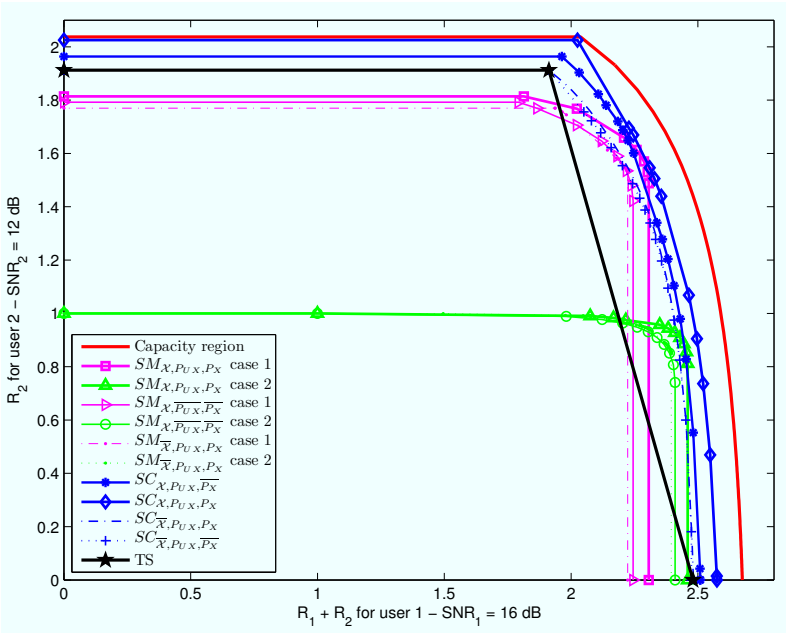

Figure 8: Achievable rate regions with $M = 8$ and $(SNR_1, SNR_2) = (16dB, 12dB)$

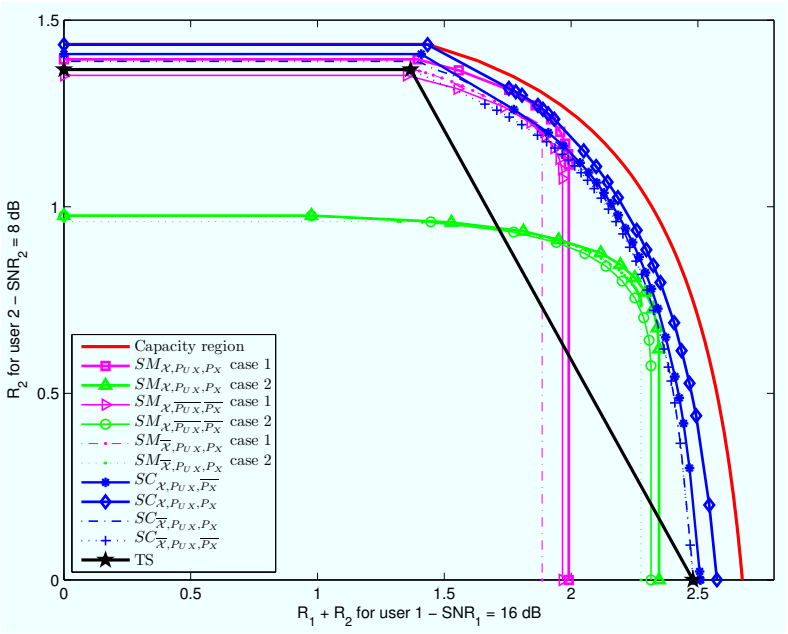

Figure 9: Achievable rate regions with $M = 8$ and $(SNR_1, SNR_2) = (16dB, 8dB)$

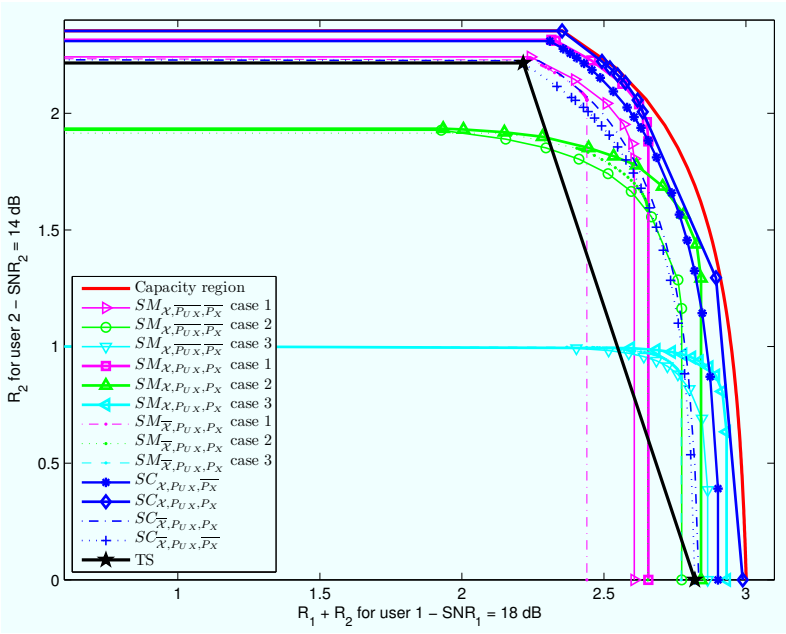

Figure 10: Achievable rate regions with $M = 16$ and $(SNR_1, SNR_2) = (18dB, 14dB)$

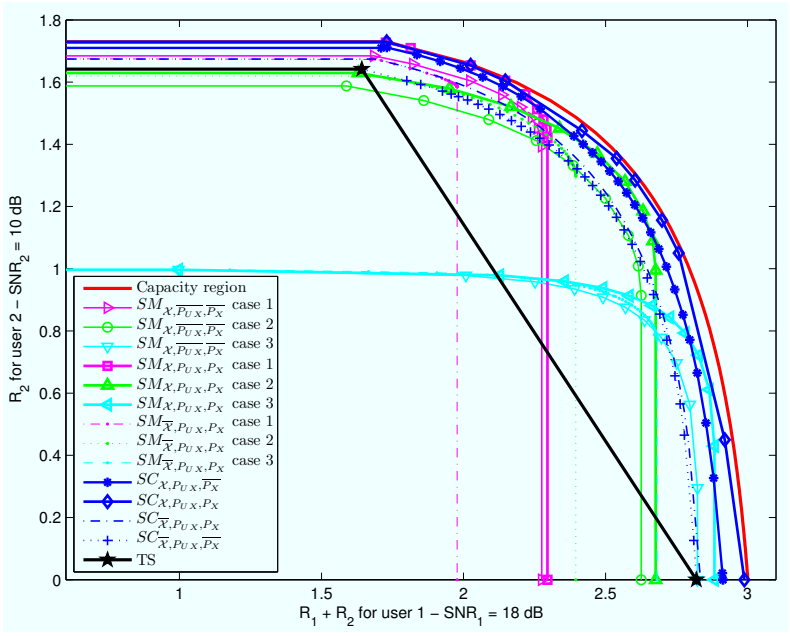

Figure 11: Achievable rate regions with $M = 16$ and $(SNR_1, SNR_2) = (18dB, 10dB)$

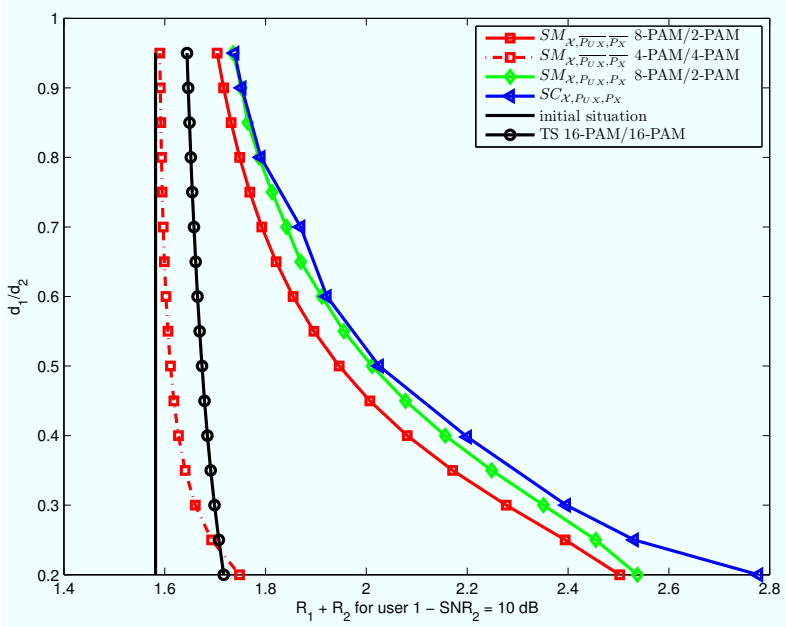

Figure 12: Coverage ratio d_1/d_2 as function of the achievable rate for user 1

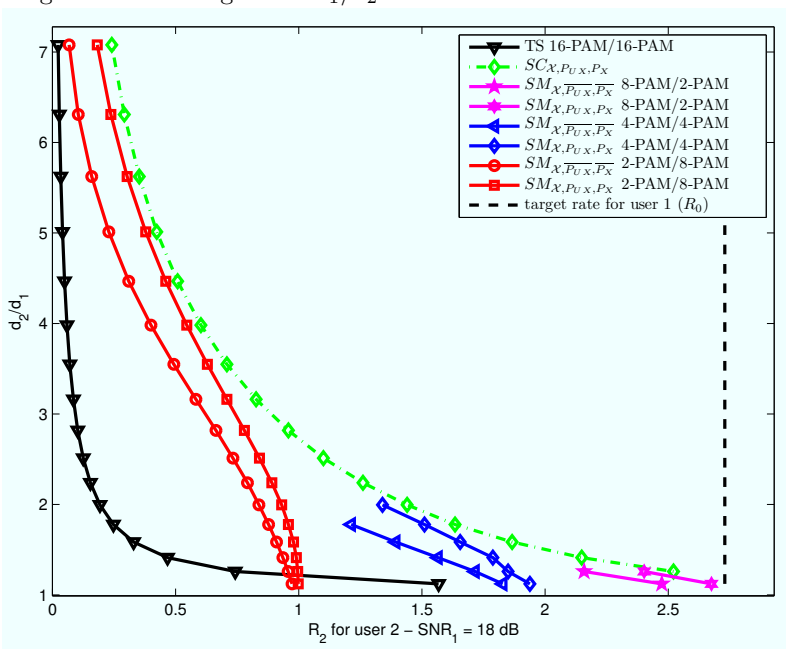

Figure 13: Coverage ratio d_2/d_1 as function of the achievable rate for user 2

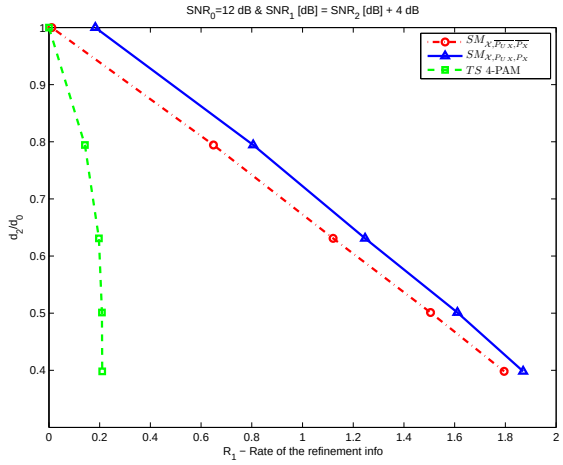

Figure 14: Reduction in legacy coverage d_2/d_0 in function of the rate of the refinement R_1.

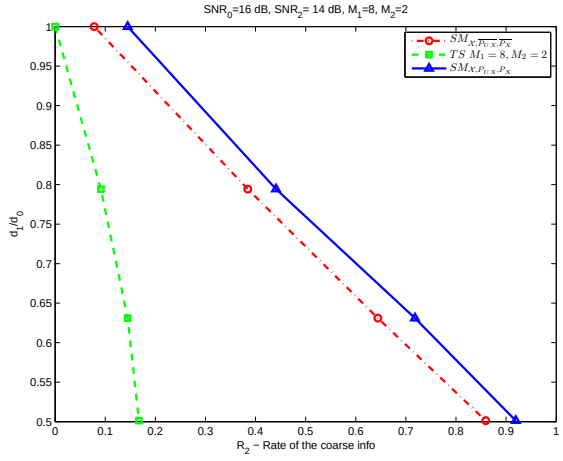

Figure 15: Reduction in legacy coverage d_1/d_0 in function of the rate of the coarse information R_2.

Annexe B

Article sur l'optimisation des débits atteignables pour les canaux de diffusion avec message confidentiel et alphabet d'entrée fini

Secrecy-Achievable Rates for the Broadcast Channel with Confidential Message and Finite Constellation Inputs

Z. Mheich, F. Alberge and P. Duhamel

Univ. Paris-Sud, UMR8506 Orsay, F-91405; CNRS, Gif-sur-Yvette, F-91192; Supélec, Gif-sur-Yvette, F-91192, 3 rue Joliot-Curie, 91192 Gif-sur-Yvette cedex, France

Tel: +33 1 69851757; fax: +33 1 69851765

e-mail:{alberge, zeina.mheich, pierre.duhamel}@lss.supelec.fr

Abstract

This paper considers the Broadcast Channel with Confidential Message (BCCM) where the sender attempts to send altogether a common message to two receivers and a confidential message to one of them. The secrecy-achievable rate regions are derived for the power-constrained Gaussian BCCM with finite input alphabet using various transmission strategies. Namely, time sharing, superposition modulation and the general case of superposition coding are used as broadcast strategies. For superposition modulation and superposition coding, the maximal secrecy-achievable rate regions are obtained by maximizing over both the constellation symbol positions and the joint probability distribution. The maximization of the secrecy rate for the wiretap channel is also studied as a particular case of the BCCM problem. We compare the considered transmission strategies in terms of the percentage of gain in achievable rates. We concentrate on the impact of the finite alphabet constraint on the achievable rates, and show that this constraint may change well known results obtained in the Gaussian case. We also study the impact of secrecy constraint on communication by comparing the secrecy-achievable rates w.r.t. the case of broadcast channel without secrecy constraint.

Index Terms

Information-theoretic security, finite-alphabet input, broadcast channel with confidential message, secrecy-achievable rate region.

I. INTRODUCTION

Security is an important issue for wireless communications. Vulnerabilities to eavesdropping comes from the shared nature of the wireless environment. Traditionally, cryptographic techniques are used at higher layers of the protocol stack for security purpose. These techniques are based on the assumption of limited computational power at the eavesdropper. Recently, the wireless communications community has devoted a considerable attention to the information theoretic security at the physical layer, which makes use of totally different concepts. Indeed, in physical layer security, secrecy is achieved by exploiting the randomness of the wireless channels and does not assume any computational restrictions at the eavesdropper.

In the wiretap channel model, introduced by Wyner in [1], a transmitter wants to send reliably confidential message to a legitimate receiver and to keep the transmitted messages secure from an eavesdropper. The level of ignorance at the wiretapper with respect to the confidential message is measured by the equivocation rate. Wyner demonstrated that secure communication is possible without sharing a secret key and determined the secrecy capacity of the memoryless degraded wiretap channel. The secrecy capacity is the maximal achievable rate to communicate reliably with the destination while the wiretapper is not able to obtain any information from the incoming signal. The secrecy capacity for the Gaussian wiretap channel was given later in [2]. Csiszar and Korner studied in [3] a more general model of the wiretap channel called broadcast channel with confidential message where the channels do not obey necessarily any degradation relationship. In this model, there is a common message for two receivers in addition to the confidential message for one receiver. More recently, fading was also introduced in the secret transmission model [4],[5] and the Gaussian MIMO and MISO wiretap channel are revisited in [6] and [7] respectively.

The secrecy capacity for the Gaussian wiretap channel and the secrecy capacity region for the Gaussian BCCM are achieved using random Gaussian codebook. However, Gaussian alphabets are not used in real systems since they are not practical to implement, instead finite constellations such as M-PAM, M-QAM are considered, usually with equal probability. The impact of finite size constellation on the secrecy achievable rate is analyzed in [8] and [9] in the particular case of

equiprobable symbols. It is shown that the secrecy rate curves for a finite constellation plotted against the SNR and for a fixed noise variance of the eavesdropper's channel have a global maximum at an internal point. This comes in contrast to what is known in the case of Gaussian codebook input where the secrecy capacity curve is a bounded, monotonically increasing function of SNR. Ref. [10] investigates the secrecy rate of the Gaussian wiretap channel with standard M-PAM inputs. The authors provide the necessary conditions for both the M-PAM input power and the M-PAM input distribution to maximize the secrecy rate which they specialize to the asymptotic low-power and high-power regimes. Ref. [11] and [12] study the effect of finite discrete-constellation on the achievable secrecy rate of multiple-antenna wiretap channels and [13] investigates the power allocation and artificial noise design for OFDM wiretap channels with discrete channel inputs.

This paper studies the achievable rates for the Gaussian broadcast channel with confidential message using M-PAM constellations. We determine the maximal secrecy-achievable rate region for Gaussian BCCM, by optimizing over both symbol positions and the joint probability distribution, subject to the availability of a suitable initial guess. The symbol positions in our work are allowed to take arbitrary values and are not necessarily proportional to those of standard constellation as in [10]. This leads to the determination of the maximal secrecy-achievable rates with any constellation of M symbols. The secrecy achievable rate regions are also given for various broadcast transmission strategies which differ in their complexity of implementation. Preliminary and partial results were published in [14] by the same authors. The whole picture is given here. Additional contributions of this paper compared to [14] are specified hereafter. Regarding the secrecy-achievable rate regions for the BCCM, comparisons between the various strategies are conducted, in this paper, in terms of SNR savings for target achievable rates and percentage of gain in achievable rates. The corresponding trade-off between complexity and efficiency is discussed. The goal is to know whether using practical schemes is sufficient to achieve good rates or it leads to significant losses. Moreover, the impact of secrecy constraint is also studied in this paper by analyzing the secrecy gap, between the maximal secrecy-achievable rate region and the maximal achievable rate region for the Gaussian broadcast channel without secrecy constraint, which gives an idea about the portion of the private message rate for some user that can be secured. This contribution is a first step towards a practical implementation of secure communication at the physical layer.

II. ACHIEVABLE RATES FOR THE BCCM

A. General case : BCCM

This section recalls classical results on the achievable rates of the BCCM [3], i.e. a broadcast channel with two receivers for which a sender attempts to send two messages simultaneously: a common message w_0 to both receivers and a secret message w_1 for receiver 1. A discrete-memoryless BCCM (DM-BCCM) consists of an input alphabet $\mathcal{X}$, two output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$ and transition probabilities $P_{Y_1Y_2|X}$ such that $P_{Y_1^nY_2^n|X^n}(y_1^n, y_2^n|x^n) = \prod_{i=1}^n P_{Y_1Y_2|X}(y_{1i}, y_{2i}|x_i)$ (Figure 1). Conventionally, random variables (RV) are written in upper case letters and particular realizations are written in corresponding lower case letters.

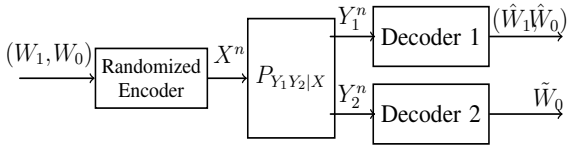

Figure 1. The broadcast channel with confidential message

A $(2^{nR_0}, 2^{nR_1}, n)$ code for the DM-BCCM consists of the following elements.

- Two message sets $\mathcal{W}_0 = \{1, .., 2^{nR_0}\}$ and $\mathcal{W}_1 = \{1, .., 2^{nR_1}\}$. We assume throughout that the messages W_0 and W_1 are uniformly distributed over the message sets $\mathcal{W}_0$ and $\mathcal{W}_1$ respectively.
- A randomized encoder that maps a message pair $(w_0, w_1) \in (\mathcal{W}_0, \mathcal{W}_1)$ to a codeword x^n.
- Two decoders: Decoder 1 maps a received sequence $y_1^n \in \mathcal{Y}_1^n$ to a message pair $(\hat{w}_0, \hat{w}_1)$ or an error message e, the second one at receiver 2 maps a received sequence $y_2^n \in \mathcal{Y}_2^n$ to a message $\tilde{w}_0$ or an error message e.

The secrecy level of W_1 at the eavesdropper is measured by the *equivocation rate*. The average error probability is $P_e^{(n)}$ with expression given below

$$\frac{1}{2^{nR_0}2^{nR_1}} \cdot \sum_{w_0=1}^{nR_0} \sum_{w_1=1}^{nR_1} \Pr\{(\hat{w}_0, \hat{w}_1) \neq (w_0, w_1) \text{ or } \tilde{w}_0 \neq w_0\}$$

The rate-equivocation triple (R_0, R_1, R_e) is achievable if there is a sequence of $(2^{nR_0}, 2^{nR_1}, n)$ codes with $P_e^{(n)} \to 0$ as $n \to \infty$ and with equivocation rate satisfying $R_e \leq \liminf_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n)$.

Throughout this work, we focus on the case in which *perfect secrecy* is achieved ($R_1 = R_e$) , i.e. the confidential messages transmitted are entirely hidden to the eavesdropper. The secrecy capacity region is the set of all rate pairs (R_0, R_1) such that $(R_0, R_1, R_e = R_1)$ is achievable. The secrecy capacity region which has been provided in [3] is the closure of the set that includes all (R_0, R_1) such that:

$$0 \leq R_1 \leq I(V;Y_1|U) - I(V;Y_2|U) \tag{1}$$

$$R_0 \leq \min\{I(U;Y_1), I(U;Y_2)\} \tag{2}$$

for some $P_{UVXY_1Y_2}$, and where U and V are auxiliary random variables satisfying $U \leftrightarrow V \leftrightarrow X \leftrightarrow Y_1Y_2$. U serves as a cloud center distinguishable by both receivers. In other terms, it carries the common information. V is an auxiliary random variable for additional randomization at the encoder side. The cardinality of the set $\mathcal{U}$ can be limited to $|\mathcal{U}| \leq |\mathcal{X}| + 3$.

The channel to receiver 2 is called a physically degraded version of the channel to receiver 1 if $p(y_1, y_2|x) = p(y_1|x)p(y_2|y_1)$ i.e. $X \leftrightarrow Y_1 \leftrightarrow Y_2$ is a Markov chain. In this case, it is shown in [4] that $I(V;Y_1|U) - I(V;Y_2|U) \leq I(X;Y_1|U) - I(X;Y_2|U)$. Moreover, we have $I(U;Y_1) \geq I(U;Y_2)$ due to the Markov chain condition $U \leftrightarrow V \leftrightarrow X \leftrightarrow Y_1 \leftrightarrow Y_2$. Thus, the achievable rates in (1) and (2) satisfy for the degraded BCCM $U \leftrightarrow V \leftrightarrow X \leftrightarrow Y_1 \leftrightarrow Y_2$ [4]:

$$R_1 \leq I(X;Y_1|U) - I(X;Y_2|U) \tag{3}$$

$$R_0 \leq I(U;Y_2) \tag{4}$$

where $V = X$ in this case. It can be shown that the secrecy capacity region depends only on the conditional marginals. Hence, this result generalizes to stochastically degraded DM-BCCM. In the case of degraded BCCM, the cardinality of $\mathcal{U}$ can be limited to $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$ which follows from Caratheodory's theorem [15]. Comparing to the capacity region of the degraded broadcast channel without confidential messages [16], it may seem that the secrecy constraint leads to sacrifice a significant portion of the available capacity to confuse the eavesdropper. However, this is misleading because it is possible to send an additional private message to the legitimate receiver in addition to the confidential message to achieve the capacity region of the degraded broadcast channel without confidential message. In this paper, we will focus on the study of the secrecy rate for the legitimate receiver and the common message rate only.

Throughout this work, we consider the (degraded) Gaussian BCCM channel. The channel outputs are $Y_i = X + Z_i$, where $i \in \{1, 2\}$, $Z_i \sim \mathcal{N}(0, N_i)$ and $N_2 > N_1$. We consider also an input power constraint $\mathbf{E}[X^2] \leq P$. In [4], the secrecy capacity region of the Gaussian BCCM with input power constraint P is given as:

$$= \bigcup_{\beta \in [0,1]} \left\{ (R_0, R_1) : \begin{array}{l} R_0 \leq C(\frac{(1-\beta)\cdot P}{N_2 + \beta \cdot P}) \\ \\ R_1 \leq C(\frac{\beta \cdot P}{N_1}) - C(\frac{\beta \cdot P}{N_2}) \end{array} \right. \tag{5}$$

where $C(x) = \frac{1}{2} \cdot \log_2(1 + x)$. The achievability of the secrecy-capacity region follows from the previous definition of achievable rates for degraded BCCM with the following choice of random variables: $U \sim \mathcal{N}(0, (1 - \beta) \cdot P)$, $X = U + X'$ with $X' \sim \mathcal{N}(0, \beta \cdot P)$.

B. Wiretap channel

Now we turn to a special case of BCCM called wiretap channel (WTC) where there is no common message $(R_0 = 0)$. The secrecy capacity of the discrete memoryless WTC is obtained by taking $U = const$ in the BCCM case [3]. Thus, by replacing $U = const$ in (1), the secrecy capacity of the DM-WTC is

$$R_1 = \max_{P_{VX}} I(V; Y_1) - I(V; Y_2) \tag{6}$$

As a generalization of the concept of "degradation" in broadcast channels, [17] introduced two weaker partial ordering of "more capable" and "less noisy" . The single letter characterization of the relation " channel 1 is more capable than channel 2" was that for all P_X, $I(X; Y_1) \geq I(X; Y_2)$. The relation "channel 1 is less noisy than channel 2" was single-letter characterized by the property that for every $V \to X \to Y_1 Y_2$

$$I(V; Y_1) \geq I(V; Y_2) \tag{7}$$

In [17], it was shown that the " more capable" condition is strictly weaker than the "less noisy" condition which is, in turn, strictly weaker than " channel 2 is a degraded version of channel 1". It can be shown that when channel 1 is less noisy than channel 2 i.e., if condition 7 holds then, $I(V; Y_1) - I(V; Y_2) \leq I(X; Y_1) - I(X; Y_2)$. Thus the secrecy capacity in this case is obtained from (6) by taking $V = X$ [3], i.e.

$$R_1 = \max_{P_X} I(X; Y_1) - I(X; Y_2) \tag{8}$$

The secrecy rate in (8) holds also under the weaker condition that channel 1 is more capable than channel 2. We note that the wiretap channel was introduced by Wyner in [1] who assumed that the channel to the eavesdropper is a physically degraded version of the channel to the legitimate receiver and thus the secrecy capacity is given in (8).

The secrecy capacity of the Gaussian wiretap channel has been provided in [2] and can be obtained (when $N_2 > N_1$) from (5) by taking $\beta = 1$ (the total available power is used to transmit the confidential message):

$$R_1 = C\left(\frac{P}{N_1}\right) - C\left(\frac{P}{N_2}\right) \tag{9}$$

It is achieved using Gaussian random codes where $X \sim \mathcal{N}(0, P)$.

Obviously, as can be seen by comparing (8) and (3), the wiretap channel is a special case of BCCM where U is a constant, and R_0 is equal to zero.

III. Broadcast Transmission Strategies

The common rate R_0 in (4) and the secrecy rate R_1 in (3) are achieved using superposition coding (SC) scheme to transmit simultaneously both messages. A stochastic encoding [3], [18] is used to ensure security. This paper considers various broadcast strategies which differ in their complexity of implementation and performance. A detailed description of these strategies can be found in [19], [20]. These strategies are listed below in ascending order of complexity and performance:

- Time Sharing (TS). Messages w_0 and w_1 are transmitted in different time-slots. Within a slot the system is equivalent to a classical point-to-point communication. Here, transmitted symbols belong to a standard M-PAM constellation ($\mathcal{X} = \{M - 1 - 2 \cdot (i-1) \quad \text{for } i = 1, .., M\}$).
- Superposition Modulation (SM) M symbols are obtained by adding two random variables X_1 and X_2 of respective cardinality M_1 and M_2, i.e. $M = M_1 M_2$. This corresponds to a separable labeling. Two schemes are considered: (i) equiprobable symbols and optimized symbol positions, denoted as $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$, and (ii) full optimization of symbol positions and joint probability distribution P_{UX}, a scheme denoted as $SM_{\mathcal{X},P_{UX},P_X}$. The first scheme $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ allows a separate encoding for both common and secret information.

- SUPERPOSITION CODING (SC). P_{UX} takes the most general form, i.e. U has the largest cardinality: $|\mathcal{U}| = |\mathcal{X}|$ for Gaussian BCCM. The auxiliary variable U serves as a cloud center for the information. Thus labeling does not allow to distinguish between the common and the secret information. The encoding of both messages is done jointly using the joint distribution of probability P_{UX} and the decoding is based on large block typicality [21]. Superposition coding is here assumed to correspond to the optimization of the symbol position and P_{UX}. This scheme is denoted as $SC_{\mathcal{X},P_{UX},P_X}$.

IV. ACHIEVABLE RATES WITH M-PAM

The secrecy capacity region of the Gaussian BCCM is achieved using Gaussian input alphabets. However, practical systems usually use finite size constellation whose symbols are chosen with equal probability to transmit information for users. This section shows how to compute the maximal secrecy-achievable rate region (i.e. R_0 as a function of R_1) of two-user power-constrained (degraded) Gaussian BCCM when the transmitted signal is modulated using an M-PAM constellation. [1]

A. Problem Formulation

We consider a Gaussian BCCM system model in which the transmitter attempts to send a common message to two receivers (1 and 2) and a confidential message to receiver 1 at rates R_0 and R_1 respectively. The AWGN channel of receiver $k \in \{1, 2\}$ follows a normal distribution of zero mean and variance N_k. The channel input X is subject to a practical average power constraint $\mathbb{E}[X^2] \leq P$. We assume also an input alphabet $\mathcal{X}$ consisting of M real valued symbols : $|\mathcal{X}| = M$. We study the case where the receiver SNRs verify $SNR_2 < SNR_1$, with $SNR_k = \frac{P}{N_k}$, which means that the output at receiver 2 is a degraded version of the output at receiver 1. The optimal rates R_0 and R_1 for some broadcast strategy satisfy the right hand side inequalities of (3) and (4). Thus the achievable rates in our system model can be computed for some $\theta \in [0, 1]$,

[1]This work can be extended to complex Gaussian channel models using M-PSK and M-QAM constellations.

by solving the following weighted sum rate maximization problem:

$$\begin{aligned} \max_{P_{UX},\mathcal{X}} \quad & \theta \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U)\Big] + (1-\theta)\cdot I(U;Y_2) \\ s.t. \quad & \begin{cases} p_{ij} \geq 0 \quad \forall (i,j) \in \mathcal{I}\times\mathcal{J} \\ \sum_{ij} p_{ij}\cdot x_j^2 \leq P \\ \sum_{ij} p_{ij} = 1 \end{cases} \end{aligned} \tag{10}$$

where $p_{ij} = \Pr\{U = u_i, X = x_j\}$, $j \in \mathcal{J} = \{0,..,M-1\}$ and $i \in \mathcal{I} = \{0,..,|\mathcal{U}|-1\}$. When P_X is constrained to be uniform, the last constraint is replaced by $\sum_i p_{ij} = \frac{1}{M}$. $I(X;Y_k|U)$ where $k \in \{1,2\}$, and $I(U;Y_2)$ can be written for the Gaussian channel with finite input alphabet case as [2]

$$\begin{aligned} I(X;Y_k|U) = & \sum_{i,j} \int_{-\infty}^{+\infty} p_{ij} P_{Y_k|X}(y_k|x_j)\cdot \\ & \log \frac{(\sum_{j'} p_{ij'}) P_{Y_k|X}(y_k|x_j)}{\sum_{j'} p_{ij'} P_{Y_k|X}(y_k|x_{j'})} dy_k \end{aligned} \tag{11}$$

$$\begin{aligned} I(U;Y_2) = & \sum_{i} \int_{-\infty}^{+\infty} (\sum_{j} p_{ij} P_{Y_2|X}(y_2|x_j))\cdot \\ & \log \frac{\sum_{j'} p_{ij'} P_{Y_2|X}(y_2|x_{j'})}{(\sum_{j'} p_{ij'})(\sum_{i',j'} p_{i'j'} P_{Y_2|X}(y_2|x_{j'}))} dy_2 \end{aligned} \tag{12}$$

Here also, one can note that the optimization for the wiretap channel (8) is equivalent to the one for BCCM with $\theta = 1$ and constant U (10).

Clearly, it is difficult to solve the non-concave problem (10) using exhaustive search method especially when M increases. An iterative method is proposed in the next section

B. Numerical Solution

In order to solve the problem (10), we use an alternative maximization of the Lagrangian with respect to $\mathcal{X}$ and P_{UX}. A similar method was proposed in [19] for the broadcast channel without secrecy constraint. The Lagrangian L of problem (10) can be written as:

$$\begin{aligned} L(P_{UX},\mathcal{X},s) = & \theta \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U)\Big] \\ & + (1-\theta)\cdot I(U;Y_2) + s\cdot\Big(P - \sum_{ij} p_{ij}\cdot x_j^2\Big) \end{aligned} \tag{13}$$

[2]All logarithms are taken base 2.

For a given value of s, the maximization of L with respect to P_{UX} and to $\mathcal{X}$ is done iteratively until convergence:

$$P_{UX}^{(\ell)} = \arg \max_{P_{UX} \in \mathcal{C}} L(P_{UX}, \mathcal{X}^{(\ell-1)}, s) \tag{14}$$

$$\mathcal{X}^{(\ell)} = \arg \max_{\mathcal{X}} L(P_{UX}^{(\ell)}, \mathcal{X}, s) \tag{15}$$

where ℓ is the iteration index and $\mathcal{C}$ denotes the set of constraints on P_{UX} and can be defined either as $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$ or as $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i} p_{i,j} = \frac{1}{M}\}$ if symbols are used with equal probability. It is observed in [14] that $L(P_{UX}^{(\ell)}, \mathcal{X}, s)$ is a concave function in $\mathcal{D}$ where $\mathcal{D}$ is the set of input alphabets with a minimum spacing between symbols greater than d and d is a function of the SNR and of the constellation size [14]. A simplex method is then used to solve (15) on $\mathcal{D}$.

Now, we turn to the optimization problem in (14) which is used when P_{UX} is not constrained to be uniform. In the literature, there exists a Blahut-Arimoto type algorithm which enables to maximize the secrecy rate $R_1 = I(X;Y_1) - I(X;Y_2)$ for the case of wiretap channel in which the eavesdropper's channel is noisier than the main channel. This algorithm proposed in [22] is guaranteed to converge to a global maximum since the function $I(X;Y_1) - I(X;Y_2)$ is concave in P_X for a fixed $\mathcal{X}$ in this case [23]. For the general case of Gaussian BCCM, the following lemma focuses on the (non)-concavity of (14) when $0 \leq \theta < 1$.

Lemma 1: (i) The receiver 1's channel $X \rightarrow Y_1$ is less noisy than the receiver 2's channel $X \rightarrow Y_2$ if and only if $I(X;Y_1|U) - I(X;Y_2|U)$ is a concave function of P_{UX}, (ii) $I(U;Y_2)$ is a difference of concave functions of P_{UX}.

Proof: (i) is proven in the Appendix and (ii) is demonstrated in [24, Appendix A]. ■

Thus (14) is a non-concave optimization problem but it is similar to the non-concave problem without secrecy constraint considered in [19]. From the expressions of the mutual information $I(X;Y_k|U)$ and $I(U;Y_2)$, where $k \in \{1,2\}$, we have also the following lemma.

Lemma 2: Consider the case of superposition coding where the alphabet of the transmitted signal is not a sum of two alphabets for the common and the secret information respectively. In this case, if $P_{UX}^{*(l)}(s)$ is a solution of problem (14), then any joint probability distribution P_{UX} obtained by permuting the rows of $P_{UX}^{*(l)}(s)$ is also a solution of problem (14).

Proof: Lemma 2 comes from (11), (12) and the constraints in (10) in which permuting the rows of the joint distribution of probability does not change the function value in (14).

Hence, problem (14) has multiple solutions. However Lemma 2 does not hold for superposition modulation, since in this scheme $\mathcal{U}$ represents the alphabet of the common information. Thus the constellation symbol positions in $\mathcal{X}$ will depend on the values of $\mathcal{U}$, i.e. $X = U + X_1$ where X_1 represents the signal carrying the secret information. Consequently, permuting the rows of P_{UX} will change the mutual information values in (11), (12) for superposition modulation strategy. ■

Therefore, obviously, in some of the considered situations, the problem of interest has multiple solutions, and the uniqueness of a global maximum cannot hold. This is indicated below.

In order to solve the optimization problem in (14) with constraint set $\mathcal{C}$ we used a Blahut-Arimoto type algorithm which can be done for the Gaussian BCCM using the same method in [25] for the degraded broadcast channel without secrecy constraint. However since (14) is not concave in P_{UX}, the Blahut-Arimoto type algorithm can be demonstrated to converge only when some specific conditions hold [25]. These conditions are given in theorem 2 of [25]. Indeed, if the solution of (14), $P_{UX}^{*(l)}(s)$, lies in a set $T_{k,\theta}(\tilde{P}_{UX})$ and the function $L(P_{UX}, \mathcal{X}^{(\ell-1)}, s)$ is concave in $T_{k,\theta}(\tilde{P}_{UX})$ and the initial guess $P_{UX}^{(0)(l)}(s) \in T_{k,\theta}(\tilde{P}_{UX})$, the Blahut-Arimoto type algorithm is shown to converge to the optimal value. $T_{k,\theta}(\tilde{P}_{UX})$ is defined in [25] as the set of all the points $P_{UX} \in S_{k,\theta} \triangleq \{P_{UX} | L(P_{UX}, \mathcal{X}^{(\ell-1)}, s) \geq k\}$ such that P_{UX} is reachable from $\tilde{P}_{UX} \in S_{k,\theta}$ by a continuous path. Therefore, the problem is now to choose an appropriate initial point. It is observed in [14] that the size of the region $T_{k,\theta}(\tilde{P}_{UX})$ where the objective function in (14) is concave in P_{UX} is larger when θ increases. Thus we have more chance that the algorithm converges from a random initial guess in this case. In our experiments, the initial guesses are chosen randomly (avoiding "Degenerate cases" such as uniform distribution and distribution with similarities [14]) and the Blahut-Arimoto type algorithm is observed to converge to reasonable solutions, since the resulting secrecy regions have a very smooth shape. In the case of general superposition coding, the algorithm converges to one of the $M!$ solutions (lemma 2). Note that when $\theta = 0$, the maxima of $I(U; Y_2)$ are obtained when $U \equiv X$. Note also that the algorithm proposed in [22] is a particular case of the Blahut-Arimoto type algorithm for the Gaussian BCCM when $\theta = 1$.

Clearly, each iteration of the alternative maximization method increases the objective function. In the experiments, we have observed that this method converges at least to a local maximum (denoted $p_{i,j}^*(s)$, $x_j^*(s)$, $0 \leq j \leq M-1$, $0 \leq i \leq |\mathcal{U}| - 1$). Finally, in order to update the value

of s, we use a gradient search method as follows:

$$s^{(k+1)} = \Big[s^{(k)} - \beta\Big(P - \sum_{i,j} p_{ij}^{*}(s^{(k)}) \cdot (x_j^{*}(s^{(k)}))^2\Big)\Big]^{+} \tag{16}$$

where $[.]^{+} = \max(., 0)$. The algorithm used to solve the optimization problem (10) is summarized in Table I.

Step 0	$s \leftarrow s^{(0)}$	
Step k	Step 0	$\mathcal{X} \leftarrow \mathcal{X}^{(0)}$ where $\mathcal{X} = (x_0, x_1, .., x_{M-1})$
	Step ℓ	$P_{UX}^{(\ell)} = \arg\max_{P_{UX} \in \mathcal{C}} L(P_{UX}, \mathcal{X}^{(\ell-1)}, s^{(k-1)})$ $\mathcal{X}^{(\ell)} = \arg\max_{\mathcal{X}} L(P_{UX}^{(\ell)}, \mathcal{X}, s^{(k-1)})$
	Stopping criterion	$\lvert L(P_{UX}^{(\ell)}, \mathcal{X}^{(\ell)}, s^{(k)}) - L(P_{UX}^{(\ell-1)}, \mathcal{X}^{(\ell-1)}, s^{(k-1)})\rvert \leq \epsilon_L$
	$s^{(k)} = \Big[s^{(k-1)} - \beta\Big(P - \sum_{i,j} p_{ij}^{*}(s^{(k-1)}) \cdot (x_j^{*}(s^{(k-1)}))^2\Big)\Big]^{+}$ where $[.]^{+} = \max(., 0)$	
Stopping criterion	$\lvert s^{(k)} - s^{(k-1)}\rvert \leq \epsilon_s$	

Table I

NUMERICAL SOLUTION FOR SOLVING (10)

V. RESULTS AND DISCUSSION

This section provides an evaluation of the secrecy achievable rate regions for Gaussian BCCM using various transmission strategies. A comparison between the secrecy achievable rate regions for Gaussian BCCM using time sharing, superposition modulation and superposition coding is provided. The effect of constellation shaping is evaluated by analyzing the secrecy-achievable rate region curves obtained for an M-PAM constellation ($M \in \{4, 8, 16\}$) and for several pairs (SNR_1, SNR_2). The comparisons of secrecy-achievable rates are conducted in terms of SNR savings for target achievable rates (Maximum Shaping Gain) and in terms of Maximum Percentage of Gain on the common message rate R_0 or the secrecy message rate R_1 or the sum $R_0 + R_1$. These quantities are defined below.

Definition 1: Consider two transmission strategies (A and B). The pair of rates (R_1, R_0) is achieved for (SNR_1, SNR_2) with A and for $(SNR_1 + \Delta SNR, SNR_2 + \Delta SNR)$ with B. The

shaping gain (with A compared to B) is ΔSNR. The maximum shaping gain is defined as:

$$MG_{SNR_{dB}}(A|B) = max_{R_0}\Delta SNR \tag{17}$$

The maximum percentage of gain on the secrecy message rate is defined below and can be defined in the same way for the other cases.

Definition 2: Consider two transmission strategies (A and B). For a given pair of SNR (SNR_1, SNR_2) and a fixed value of R_0, the achievable pair of rates is (R_1^A, R_0) resp. (R_1^B, R_0) with A resp. B. The gain on the secrecy achievable rate for user 1 is given by

$$G_{R_1}(A|B) = \frac{R_1^A - R_1^B}{R_1^B} \cdot 100 \ (\%) \tag{18}$$

The maximum gain on the secrecy achievable rate for user 1 (with A compared to B) is given by

$$MG_{R_1}(A|B) = max_{R_0}G_{R_1}(A, B) \tag{19}$$

A. Analysis of the secrecy rate

To understand the behavior of the achievable rate region curves, we start by analyzing the secrecy rate for the wiretap channel, i.e. BCCM when $U = const.$ ($\theta = 1$). The conclusions obtained here are also applied in the presence of the common message as shown in the next section.

Figures 2 and 3, show the achievable secrecy rate using standard M-PAM constellations whose symbols are used with equal probability, where $M \in \{2, 4, 8, 16\}$, and the secrecy capacity achieved using Gaussian input. The secrecy rate is plotted in Fig. 2 and 3 as a function of SNR_1, where the eavesdropper channel SNR is 2 dB and 10 dB respectively below SNR_1. Obviously, the secrecy rate should increase when the gap between SNR_1 and SNR_2 increases for fixed SNR_1. This is in line with the results in [8],[9] where it is shown that when a standard finite constellation of M symbols is used and when symbols are chosen with equal probability, the optimal transmission power may not be given by the total available power, since when $P \to \infty$, both $I(X; Y_1)$ and $I(X; Y_2)$ converge to $\log_2 M$. An illustration is given in Fig. 2 and 3. When the SNR for both receivers is "high", the secrecy rate is null. Thus, the transmitter should use a cardinality M when the SNRs are good in order to obtain sufficient secrecy capacity.

Figure 4 gives an evaluation of the improvement in secrecy capacity obtained when relaxing the constraints of uniform symbol probability and standard positions. The secrecy rate is plotted

as a function of SNR_1 when SNR_2 is fixed to 0 dB and for $M = 4, 8, 16$. For each value of M, the secrecy rate is calculated when a standard constellation (standard positions and uniform probability) is used and compared to the case in which both the symbol positions and their probabilities are jointly optimized. We observe that the optimization of symbol positions and of their probabilities leads to significant gains when SNR_1 increases for fixed SNR_2. Indeed, when SNR_1 increases, $I(X;Y_1)$ tends to $\log_2 M$. Thus the secrecy rate $R_1 = I(X;Y_1) - I(X;Y_2)$ tends to $\log_2 M - i_2$ where $i_2 = I(X;Y_2)$ when the input alphabet belongs to a standard M-PAM and when the SNR is equal to 0 dB. However, when we optimize the symbol positions and the distribution P_X, the transmitter should not use the maximal average power allowed. Thus when SNR_1 increases, the sender may use a constellation whose symbol positions are close to the origin and to each others, while $I(X;Y_1)$ still achieve $\log_2 M$ since SNR_1 is very high. In that case, $I(X;Y_2)$ decreases because the small value of SNR_2 corresponds to a very small mutual information. Consequently, when we optimize jointly the symbol positions and their probabilities the secrecy rate converges to a value close to $\log_2 M$. For example, when $M = 4$, $SNR_1 = 33$ dB and $SNR_2 = 0$ dB, the achieved secrecy rate is equal to 1.977 bits/ch.use where the optimal symbol positions are given by $\mathcal{X} = \{0.49, 0.16, -0.16, -0.49\}$ and P_X is close to the uniform distribution. This corresponds to an optimal power equal to 0.13 even if the maximal average power allowed is equal to $P = 5$. Another illustration is given in Fig. 5. The optimal transmission power is depicted as a function of SNR_1 when SNR_2 is fixed to 0 dB and $M = 4$. We observe that when $SNR_1 \leq 11$ dB, the optimal power is given by the maximal allowed power $P = 5$. However when $SNR_1 > 11$ dB, the optimal power decreases with SNR_1.

The next subsections are concerned not only with the secrecy rate, but also with the tradeoff between the achievable common rate and the corresponding secrecy rate.

B. Superposition modulation using M-PAM

The secrecy achievable rate region computation for superposition modulation with $M = 4$ and using equiprobable symbols ($SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$) does not require to solve any optimization problem. In $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ strategy, the total power P is split such that $\alpha \cdot P$ is used for the alphabet of the secret information and $(1-\alpha) \cdot P$ for the alphabet of the common information, with $\alpha \in [0, 1]$. Thus, the four transmitted signal constellation symbols can be expressed as a function of α only [26]. Consequently, obtaining the maximal achievable rate region for $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ and

with $M = 4$, involves the computation of $I(X;Y_1|U) - I(X;Y_2|U)$ and $I(U;Y_2)$ in function of α, knowing that P_{UX} is uniform, and then to vary α between 0 and 1. In figures 6 and 7, the secrecy achievable rate regions are illustrated for the Gaussian BCCM with 4-PAM inputs using various broadcast strategies when SNR_1= 10 dB and $SNR_2 \in \{0, 8\}$ dB. In particular, for superposition modulation schemes, we observe that the maximal achievable secrecy rate is not necessarily obtained when the total power is used for the alphabet of the secret information i.e. $\alpha = 1$ which is in contrast to the case of the broadcast channel without secrecy constraint [27].

Consider for example the case where SNR_1= 10 dB and $SNR_2 = 0$ dB. Users 1 and 2 receive the secret information with a SNR equal to $SNR'_1 = \alpha \cdot \frac{P}{\sigma_1^2}$ and $SNR'_2 = \alpha \cdot \frac{P}{\sigma_2^2}$ respectively. When $\alpha = 1$, $SNR'_1 = 10$ dB and $SNR'_2 = 0$ dB, the secrecy capacity is equal to 0.51 bit/ch.use using a 2-PAM constellation according to Fig. 3. We observe also in this figure that the maximal secrecy rate is obtained when $SNR_1 = 6$ dB ($SNR_2 = -4$ dB) and is equal to 0.6711 bit/ch.use. Thus the optimal $\alpha = \alpha^*$ which maximize the secrecy rate in the case of superposition modulation is such that $\alpha^* \cdot \frac{P}{\sigma_1^2} = 6$ dB. Obviously if we solve (10) we cannot obtain the region when $\alpha > \alpha^*$ because it is not optimal, in other terms, it does not correspond to the solution of any $\theta \in [0, 1]$. This is what we can observe also from the achievable rate regions using $\{8, 16\}$-PAM.

In Fig. 12, secrecy achievable rate region with 4-PAM using $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ is given for several pairs (SNR_1,SNR_2) such that $SNR_1 - SNR_2 = 2$ dB. We observe that the maximal secrecy rate is the same for all pairs and is achieved for $\alpha < 1$ when $SNR_1 > 3$ dB. However when $SNR_1 = 3$ dB, the maximal achievable secrecy rate is when $\alpha = 1$ as $SNR_1 = 3$ dB maximizes the secrecy rate for a 2-PAM with a gap equal to 2 dB between user SNRs (see Fig. 2).

Regions of secrecy achievable rates (Fig 6 to 11) show the improvement obtained by optimizing symbol positions and the joint probabilities ($SM_{\mathcal{X},P_{UX},P_X}$ (full optimization) compared to $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ (optimization of $\mathcal{X}$ only)). In table II the maximum gain in achievable rate on R_1 or R_0 is given ($MG_{R_1}(A|B)$ or $MG_{R_0}(A|B)$), depending if the full optimization provides an horizontal or vertical gain in achievable rates. The maximum SNR savings ($MG_{SNR_{dB}}$) are also given in table II for the 4-PAM, the 8-PAM when $M_1 = 4, M_2 = 2$ and for the 16-PAM when $M_1 = 8, M_2 = 2$. For the other cases of 8-PAM ($M_1 = 2, M_2 = 4$) and 16-PAM ($M_1 = 4, M_2 = 4$ and $M_1 = 2, M_2 = 8$), we did not evaluate the gain in SNR because the maximum secrecy rate obtained by full optimization ($SM_{\mathcal{X},P_{UX},P_X}$) can not be reached by superposition modulation using equally probable symbols even when we increase the user SNRs. This is due to the fact

that in these cases and for the considered values of user SNRs, the maximum secrecy rate will not necessarily increase when the user SNRs increase as can be seen in Fig. 12. One can observe that the maximum shaping gain increases with the constellation size. Thus, constellation shaping for SM strategy seems more useful for high values of M. Moreover, we observe that independently of M, the maximum shaping gain is very small when the gap between the user SNRs increases. This is also the case for a broadcast channel model without secrecy constraints [19]. The analysis of the optimal matrix P_{UX} (results not reported) when $X = X_1 + X_2$, such that X_1 and X_2 are two signals carrying the secret information and the common information respectively, leads to the conclusion that X_1 and X_2 are not independent in general when using finite-size constellations.

C. Superposition modulation vs time sharing

This section compares the achievable rates for the Gaussian BCCM using two classical schemes: time sharing using standard constellation and superposition modulation. Moreover, we consider the case where symbols are used with equal probability for practical constraints. Figures 6-11 show that the secrecy achievable rate region can be divided into two parts, such that in each part, one strategy is more efficient than the other. This is also what is observed in [19] for a broadcast channel model without secrecy constraints. The efficiency of time sharing strategy increases with respect to superposition modulation when SNR_1 and SNR_2 become closer. Table III shows the maximum percentage of improvement in achievable rate by user 1 ($R_0 + R_1$) using $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$, comparing to TS strategy, in the achievable rate area where $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ outperforms TS. It can also be observed that the best improvement happens when δ_{SNR} increases for all $M \in \{4, 8, 16\}$. Thus superposition modulation should be preferred to time sharing when users have very different SNRs.

D. Superposition coding

It is well known that the secrecy capacity region for the Gaussian BCCM is achievable using superposition modulation scheme ($SM_{\mathcal{X},P_{UX},P_X}$), a.k.a. signal superposition, where $U = X_2$. However, in the finite-input alphabet case, the results show that the general case of superposition coding, $SC_{\mathcal{X},P_{UX},P_X}$, outperforms superposition modulation in terms of secrecy achievable rate region. A detailed discussion about this result for the two-user broadcast channel without

secrecy constraint was given in [19]. In table III, the maximum percentage of improvement in achievable rate by user 1 ($R_0 + R_1$) is given using $SC_{\mathcal{X},P_{UX},P_X}$, comparing to $SM_{\mathcal{X},P_{UX},P_X}$ (full optimization). It can be observed that the maximum gain is proportionally greater for small values of M since there is less possibilities to obtain a M-PAM via superposition modulation.

E. What is the impact of the secrecy constraint?

Let us first recall that the capacity region for a two user power-constrained Gaussian broadcast channel without secrecy constraint and with $SNR_1 > SNR_2$ is given by:

$$R_0 \leq \frac{1}{2}\log_2\left(1+\frac{(1-\beta)\cdot P}{N_2+\beta\cdot P}\right) \tag{20}$$

$$R_{p1} \leq \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_1}\right) \tag{21}$$

where R_0 is the common message rate for both receivers and R_{p1} is the private message rate dedicated for user 1 only. In the case of BCCM, the confidential message rate for user 1, R_1 is such that

$$R_1 \leq \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_1}\right) - \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_2}\right) \tag{22}$$

We observe that there is a "secrecy gap" equal to $R' = \frac{1}{2}\log_2\left(1+\frac{\beta\cdot P}{N_2}\right)$ between user 1's private message rate R_{p1} and the secrecy rate R_1. Hence, we can transmit a private message for user 1 at rate R_{p1} but only a portion of this message of rate R_1 can be secured. Equivalently, it is possible to transmit for user 1 two messages at a total rate R_{p1}: a secret message at rate R_1 and a private message at rate R' with no secrecy guaranteed. Figure 13 shows the capacity region (R_0 vs R_{p1}) and the secrecy capacity region (R_0 vs R_1) together for many pairs of user SNRs and for $M = 4$. For a fixed SNR_1, the secrecy gap increases when SNR_2 increases. For the finite alphabet case, and using the general case of superposition coding, we observe that the gap between the maximal private message rate and the maximal secrecy rate for a fixed R_0 is close to that obtained in the Gaussian alphabet case for the considered pairs of user SNRs. However when SNR_1 increases R_{p1} tends to $\log_2 M$ and thus the gap in the finite case become smaller than in the Gaussian input case. This is what we can observe in Fig. 13 for a superposition modulation scheme using equally probable symbols and with 4-PAM constellation where the maximal value of R_{p1} is equal to 1 (the maximal possible rate using a 2-PAM). Thus the gap between the maximal secrecy achievable rate region and the maximal achievable rate region

without secrecy constraint is smaller than the Gaussian alphabet case or than the case of general superposition coding for the considered pairs of user SNRs.

VI. Conclusion

In this paper, we derived the secrecy-achievable rate region for the Gaussian broadcast channel with confidential message using finite input constellations for various broadcast strategies. For superposition modulation and the general case of superposition coding, the secrecy achievable rate regions are maximized by optimizing over symbol positions and over the joint distribution of probability. It is shown that the optimal transmission power which maximizes the secrecy rate may not be given by the total available power. This is due to the fact that secrecy is obtained via a difference in available rate between users. Obviously, when the available power is such that even the worst user can decode with the maximum rate provided by the finite constellation, no secrecy can be obtained. In addition, the full maximization of secrecy-achievable rate region for superposition modulation provides more significant improvements when the cardinality of the input alphabet increases compared to the case where we optimize only symbol positions. In the case of BCCM with finite input alphabet, superposition modulation is not the optimal strategy, like in the Gaussian alphabet case. The general case of superposition coding can provide significant gains comparing to practical schemes. However in other cases, using practical schemes is sufficient to achieve good rates and provides a compromise between complexity of implementation and efficiency. Finally, we have analyzed the impact of secrecy constraint on achievable rates and we observed that the secrecy gap to confuse the eavesdropper can be important depending on users SNR.

Appendix

Proof of lemma 1 (i): First, we recall that a function $f(P_{UX})$ is a concave function of the probability distribution P_{UX} if for all $\alpha, 0 \leq \alpha \leq 1$, and all probability distributions P^a_{UX} and P^b_{UX},

$$\alpha f(P^a_{UX}) + (1-\alpha) f(P^b_{UX}) \leq f\big(\alpha P^a_{UX} + (1-\alpha) P^b_{UX}\big)$$

To prove lemma 1 (i), we use the method for proving [23, Theorem 2]. Indeed, for an arbitrary V with finite input alphabet $\mathcal{V}$, consider the Markov chain $(U,V) \to X \to (Y_1, Y_2)$. Each $v \in \mathcal{V}$

specifies a probability distribution P^v_{UX} for X in the manner

$$P^v_{UX}(u,x) = P_{UX|V}(u,x|v), \qquad (u,x) \in \mathcal{U} \times \mathcal{X}$$

We first note that

$$\begin{aligned} I(XV;Y_1|U) &\overset{i)}{=} I(X;Y_1|U) + I(V;Y_1|UX) \\ &\overset{ii)}{=} I(X;Y_1|U) \end{aligned} \tag{23}$$

where i) follows from the chain rule for mutual information and where ii) follows from the fact that $(U,V) \to X \to (Y_1,Y_2)$ is a Markov chain so that $I(V;Y_1|UX) = 0$. We note also that

$$I(XV;Y_1|U) \overset{iii)}{=} I(V;Y_1|U) + I(X;Y_1|UV) \tag{24}$$

where iii) follows from the chain rule for mutual information. By combining (23) and (24), we can write:

$$I(V;Y_1|U) = I(X;Y_1|U) - I(X;Y_1|UV) \tag{25}$$

In the same way, we can show that

$$I(V;Y_2|U) = I(X;Y_2|U) - I(X;Y_2|UV) \tag{26}$$

From (25) and (26), we infer that

$$I(V;Y_2|U) \leq I(V;Y_1|U)$$

if and only if

$$I(X;Y_1|UV) - I(X;Y_2|UV) \leq I(X;Y_1|U) - I(X;Y_2|U) \tag{27}$$

But it can be shown, using the definition of mutual information, that

$$\begin{aligned} &I(X;Y_1|UV) - I(X;Y_2|UV) \\ =&\sum_{v\in\mathcal{V}} P_V(v) \cdot \Big[I(X;Y_1|U,V=v) - I(X;Y_2|U,V=v) \Big] \\ =&\sum_{v\in\mathcal{V}} P_V(v) \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U) \Big]_{P^v_{UX}} \end{aligned} \tag{28}$$

and

$$\begin{aligned} &I(X;Y_1|U) - I(X;Y_2|U) \\ =&\Big[I(X;Y_1|U) - I(X;Y_2|U) \Big]_{\sum_{v\in\mathcal{V}} P_V(v)\cdot P^v_{UX}} \end{aligned} \tag{29}$$

Using the definition of a concave function, the part (i) of lemma 1 follows immediately from (27), (28) and (29).

ACKNOWLEDGMENT

The authors would like to thank Dr. Maël Le Treust for the helpful discussions and Prof. Pablo Piantanida for the valuable comments and suggestions to improve the quality of the paper.

REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[5] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[6] R. Liu, T. Liu, H. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1346–1359, 2013.

[7] J. Li and A. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 4, pp. 1176–1187, April 2011.

[8] G. D. Raghava and B. S. Rajan. (2010) Secrecy capacity of the gaussian wiretap channel with finite complex constellation input. [Online]. Available: http://arxiv.org/abs/1010.1163

[9] F. Renna, N. Laurenti, and H. V. Poor, "Achievable secrecy rates for wiretap OFDM with QAM constellations," in *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools, VALUETOOLS '11*, Paris, France, 2011.

[10] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On gaussian wiretap channels with M-PAM inputs," in *Wireless Conference (EW), 2010 European*, 2010, pp. 774–781.

[11] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. on communications*, vol. 60, no. 12, pp. 3816–3825, dec. 2012.

[12] ——, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *Communications Letters, IEEE*, vol. 15, no. 5, pp. 527–529, May 2011.

[13] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 6, pp. 2717–2729, June 2013.

[14] Z. Mheich, F. Alberge, and P. Duhamel, "The impact of finite-alphabet input on the secrecy-achievable rates for broadcast channel with confidential message," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Florence, Italy, May 2014.

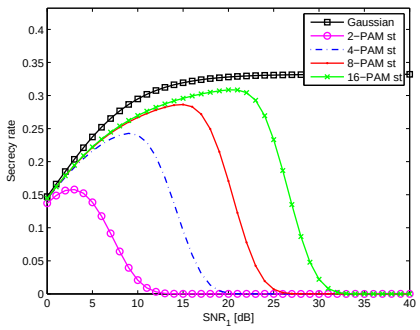

Figure 2. Secrecy rate for a Gaussian wiretap channel using Gaussian alphabet or M-PAM standard constellation where P_X is uniform. SNR_2 [dB]=SNR_1 [dB]-2 dB

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory 2nd Edition*, 2nd ed., ser. Wiley Series in Telecommunications and Signal Processing. Wiley-Interscience, Jul. 2006.

[16] T. M. Cover, "Comments on broadcast channels," *IEEE Trans. on Inform. Theory*, vol. 44, no. 6, october 1998.

[17] J. Korner and K. Marton, "Comparison of two noisy channels," in *Topics in Information Theory, Coll. Math. Soc. J. Bolyai No. 16, Ed. P. Elias and I. Csiszar*, 1977, pp. 411–423.

[18] M. Bloch and J. Barros, *Physical layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[19] Z. Mheich, F. Alberge, and P. Duhamel, "Achievable rates optimization for broadcast channels using finite size constellations under transmission constraints," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 254, 2013. [Online]. Available: http://jwcn.eurasipjournals.com/content/2013/1/254

[20] ——, "On the efficiency of transmission strategies for broadcast channels using finite size constellations," in *Proc. of the 21st European Signal Processing Conference*, Marrakech, sept. 2013.

[21] T. M. Cover, "Comments on broadcast channels," *IEEE Trans. on Inform. Theory*, vol. 44, no. 6, october 1998.

[22] K. Yasui, T. Suko, and T. Matsushima, "An algorithm for computing the secrecy capacity of broadcast channels with confidential messages," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pp. 936–940.

[23] M. van Dijk, "On a special class of broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 43, no. 2, pp. 712–714, 1997.

[24] E. Calvo, D. P. Palomar, J. R. Fonollosa, and J. Vidal, "The computation of the capacity region of the discrete degraded BC is a nonconvex DC problem," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, Toronto, Canada, July 2008.

[25] K. Yasui and T. Matsushima, "Toward computing the capacity region of degraded broadcast channel," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, June 2010, pp. 570–574.

[26] Z. Mheich, P. Duhamel, L. Szczecinski, and M.-L. Alberi-Morel, "Constellation shaping for broadcast channels in practical situations," in *Proc. of the 19th European Signal Processing Conference*, Barcelona, Spain, Aug. 2011.

[27] C. Huppert and M. Bossert, "On achievable rates in the two user AWGN broadcast channel with finite input alphabets," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, Nice, France, June 2007.

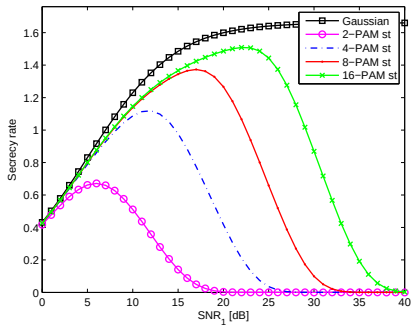

Figure 3. Secrecy rate for a Gaussian wiretap channel using Gaussian alphabet or M-PAM standard constellation where P_X is uniform. SNR_2 [dB]=SNR_1 [dB]-10 dB

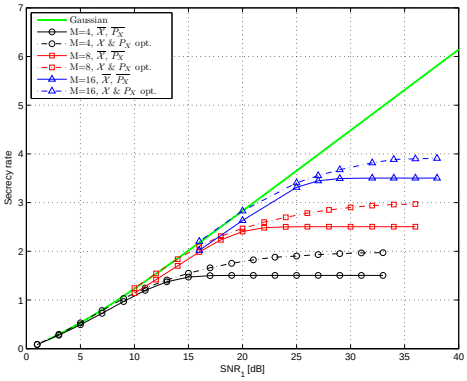

Figure 4. Maximal secrecy rate for a Gaussian WTC channel using M-PAM constellation when both symbol positions and P_X are optimized compared to standard M-PAM. $SNR_2 = 0$ dB.

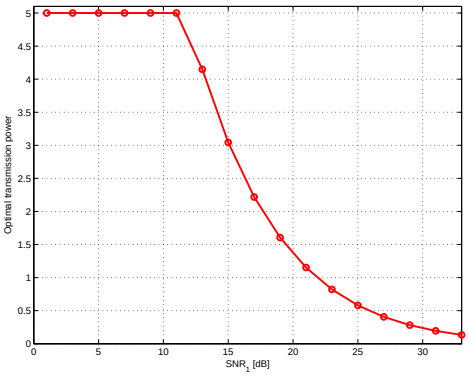

Figure 5. Optimal transmission power for a Gaussian WTC channel using 4-PAM constellation given that the maximal allowed power is equal to $P = 5$. $SNR_2 = 0$ dB.

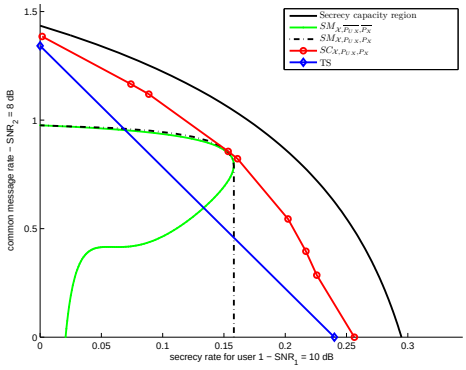

Figure 6. Secrecy achievable rate regions with $M = 4$ and $(SNR_1, SNR_2) = (10, 8)$ dB

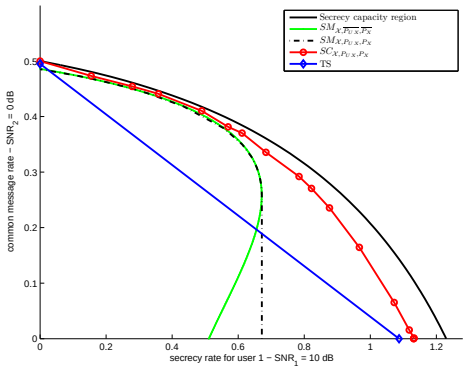

Figure 7. Secrecy achievable rate regions with $M = 4$ and $(SNR_1, SNR_2) = (10, 0)$ dB

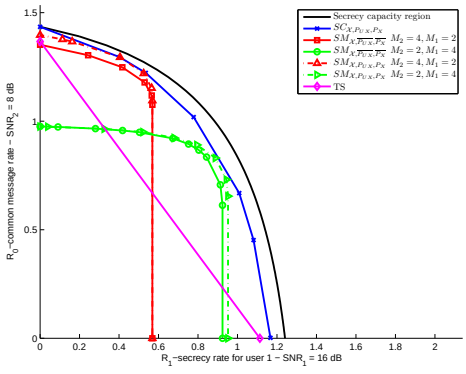

Figure 8. Secrecy achievable rate regions with $M = 8$ and $(SNR_1, SNR_2) = (16, 8)$ dB

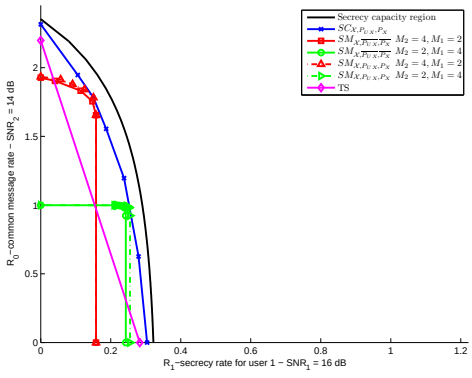

Figure 9. Secrecy achievable rate regions with $M = 8$ and $(SNR_1, SNR_2) = (16, 14)$ dB

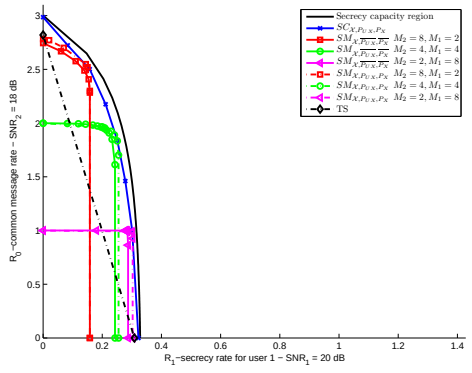

Figure 10. Secrecy achievable rate regions with $M = 16$ and $(SNR_1, SNR_2) = (20, 18)$ dB

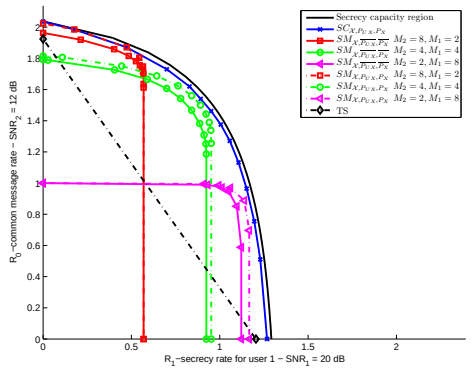

Figure 11. Secrecy achievable rate regions with $M = 16$ and $(SNR_1, SNR_2) = (20, 12)$ dB

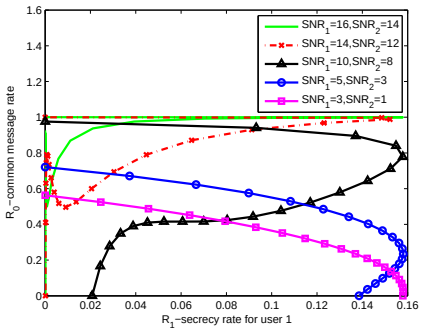

Figure 12. Secrecy achievable rate regions with $M = 4$ and for superposition modulation where symbols are used with equal probability. The SNRs are in dB.

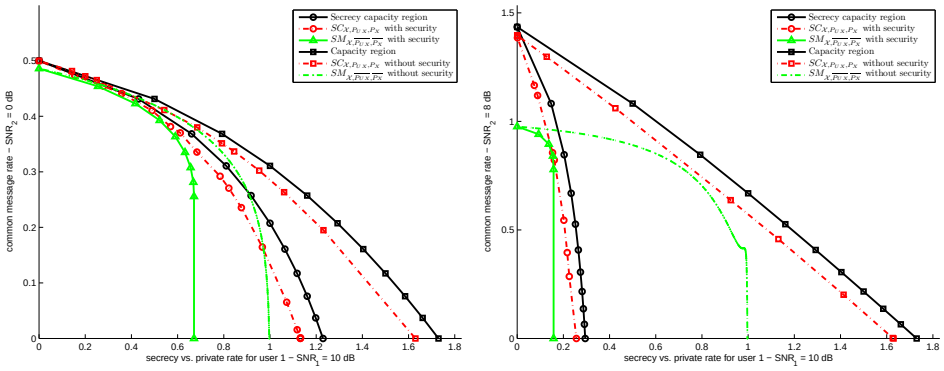

Figure 13. Maximal achievable rates for broadcast channel with finite and infinite inputs and with or without secrecy constraint.

M	SNR_1	SNR_2	$MG_{R_{0\|1}}(A\|B)$	$MG_{SNR_{dB}}(A\|B)$
4	10	8	0.06%	0.24
		6	0.477%	0.1
		4	0.34%	0.03
		2	0.14%	0
8	16	14	$5.15\%^{(M_1=4,M_2=2)}$	0.36
		12	$5.3\%^{(M_1=4,M_2=2)}$	0.43
		10	$5.14\%^{(M_1=4,M_2=2)}$	0.4
		8	$5.02\%^{(M_1=4,M_2=2)}$	0.38
16	20	18	$7.06\%^{(M_1=4,M_2=4)}$	0.61
		16	$5.93\%^{(M_1=4,M_2=4)}$	0.57
		14	$8\%^{(M_1=4,M_2=4)}$	0.54
		12	$8.48\%^{(M_1=4,M_2=4)}$	0.43

Table II

COMPARISON OF $SM_{\mathcal{X},P_{UX},P_X}$ (A) AND $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ (B) WITH RESPECT TO MG_{R_1} OR MG_{R_0} AND $MG_{SNR_{dB}}(A|B)$

M	SNR_1	SNR_2	$MG_{R_1+R_0}(A\|B)$	$MG_{R_1+R_0}(A\|C)$
4	10	8	4.51%	32.33%
		6	12.54%	11.57%
		4	24.06%	9.86%
		2	35.22%	9.7%
		0	48.23%	17.562%
8	16	14	$7.3\%^{(M_1=4,M_2=2)}$	17.48%
		12	$14.23\%^{(M_1=4,M_2=2)}$	5.4%
		10	$22.12\%^{(M_1=4,M_2=2)}$	1.03%
		8	$32.1\%^{(M_1=4,M_2=2)}$	2.99%
16	20	18	$7.09\%^{(M_1=8,M_2=2)}$	6.93%
		16	$13.73\%^{(M_1=8,M_2=2)}$	1.24%
		14	$19.94\%^{(M_1=8,M_2=2)}$	0.11%
		12	$30.31\%^{(M_1=4,M_2=4)}$	3.56%

Table III

COMPARISON OF $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ (A) VS TS (B). COMPARISON OF $SC_{\mathcal{X},P_{UX},P_X}$ (A) VS $SM_{\mathcal{X},P_{UX},P_X}$ (C).

Annexe C

Rapport technique sur l'adaptation du débit pour les protocoles HARQ sécurisés avec redondance incrémentale

Rate Adaptation for Incremental Redundancy Secure Truncated HARQ

Abstract

This paper analyzes the secrecy throughput achievable in incremental redundancy secure Hybrid ARQ (HARQ) protocol for communication over block-fading wiretap channel. The transmitter has no perfect instantaneous channel state information (CSI) but can receive an outdated version of CSI from both legitimate receiver and eavesdropper through reliable multi-bit feedback channels. Using outdated CSI, the transmitter can adapt the transmission rate. Since the transmitter cannot adapt the transmission rate to the instantaneous channel conditions, we consider the outage performance of secure HARQ protocols. We show how to find the optimal rate adaptation policies using dynamic programming framework to solve the secrecy throughput maximization problem under constraints on connection outage and secrecy outage probabilities. Numerical results for a Rayleigh-fading wiretap channel show that the rate adaptation using multilevel feedbacks provides significant gains in secrecy throughput comparing to the non-adaptive model.

I. INTRODUCTION

Automatic Repeat reQuest (ARQ), also called Automatic Repeat Query, is an error-control protocol that automatically initiates a request to retransmit any data packet or frame from the sender after detecting corrupted data. When the transmitter fails to receive an acknowledgment signal to confirm the data has been received, it usually retransmits the data and repeats the process a predetermined number of times until the transmitter receives the acknowledgment. The hybrid automatic repeat request (HARQ) protocols combine powerful channel coding with ARQ error-control to enhance the reliability of communication links. In this work we consider a powerful HARQ scheme called *incremental redundancy* HARQ where multiple sets of coded bits are generated and used in retransmissions, each representing the same data block. Thus every retransmission contains different information than the previous one. In [1], the authors provide an information-theoretic analysis of the throughput performance of HARQ protocols over block-fading Gaussian collision channels.

The security of data communication over wireless networks has become also an important concern. Due to its broadcast nature, wireless communication is susceptible to eavesdropping. Traditionally, security is implemented at the higher layers of the protocol stack by using cryptographic techniques; however these techniques rely on the assumption of insufficient computational capabilities of the eavesdroppers. In his seminal work [2], Wyner initiates the physical layer security by introducing the wiretap channel which consists of a sender which want to communicate a secret message to a legitimate receiver in the presence of an eavesdropper. Wyner assumes in his channel model that the signal received by the eavesdropper is a degraded version of the legitimate receiver signal. Then, this model was generalized in [3] where the channels do not obey necessarily any degradation relationship.

In this work, we study secure packet communication based on incremental redundancy HARQ protocols. Our work is basically inspired from [4] which investigate an information-theoretic study of HARQ protocols for a block fading wiretap channel. In the system model of [4], the transmitter obtains a 1-bit ACK/NACK feedback from the legitimate receiver to declare a successful/unsuccessful decoding via an error free public channel. The incremental redundancy protocol is considered when the sub-codewords have the same length in each retransmission. In our model, we generalize the assumptions of [4] by allowing the feedback channel to carry more bits, *i.e.* the transmitter uses multilevel feedback channel from both the legitimate receiver and the eavesdropper. Then the rate can be adapted using such a multilevel-feedback by allowing the sub-codewords length to change at each retransmission. The gains of variable rate transmission over the fixed-rate for the predefined families of code were shown in many works as in [5], [6], [7].

II. System Model and Preliminaries

A. System model

As shown in Fig.1, we consider the block fading wiretap channel where a transmitter X sends confidential messages to a legitimate receiver Y in the presence of an eavesdropper Z which listens to the transmission. Both the main channel (source-destination channel) and the eavesdropper channel (source-eavesdropper channel) experience K-block fading in which channels remain constant over a block but vary independently from block to another. At the transmitter, a confidential message w is encoded into codeword x^N of N symbols $x_1, x_2, .., x_N$.

We do not constrain N, that is, we assume that the code with arbitrarily rate can be constructed as in [5]. Any subset of the symbols x_j is called a subcodeword. The codeword x^N is divided into K subcodeword $\mathbf{x}_k$, $k = 1, .., K$. The codeword occupies K slots: for $k = 1, .., K$, the kth block $\mathbf{x}_k$ is sent in the kth slot and received by the legitimate receiver through the channel gain a_k and by the eavesdropper through the channel gain b_k.

The tth received symbol x_t in the kth block is given by:

$$y_t = a_k \cdot x_t + v_t$$

$$z_t = b_k \cdot x_t + u_t$$

where the index k indicates the block number, $t = 1, .., N$ is the index of the transmitted symbol, v_t and u_t are zero mean unit variance i.i.d. Gaussian noise of the main and eavesdropper channels respectively at the tth transmission. a_k, b_k are the fading channel coefficients of the main and eavesdropper channels respectively in the kth block. In our case, though, the channel coefficients a_k et b_k are modeled as i.i.d random variables $A_1, .., A_K$ et $B_1, .., B_K$.

We assume that the symbols of the codeword are constrained to have unit average power and are samples of a zero mean real Gaussian distribution, i.e. $\mathbb{E}[X^2] \leq 1$ where X is a random variable denoting the transmitted signal. Thus the Signal-to-Noise Ratios (SNR) received at the legitimate receiver and the eavesdropper will be respectively $h_k = a_k^2$ and $g_k = b_k^2$ at the kth transmission.

We consider the setting where the transmitter has no instantaneous channel state information available from either the main channel or the eavesdropper channel, but only channel statistics. For each channel (main channel or eavesdropper channel), the constant gain during each block is assumed to be perfectly known at the respective receiver but unknown at the transmitter.

We will consider Rayleigh block fading, thus the main channel instantaneous SNR, h and the eavesdropper instantaneous SNR, g are characterized by two exponential probability distribution functions:

$$p_H(x) = \frac{1}{\overline{h}} \cdot e^{-\frac{x}{\overline{h}}} \tag{1}$$

$$p_G(x) = \frac{1}{\overline{g}} \cdot e^{-\frac{x}{\overline{g}}} \tag{2}$$

where $\overline{h}$ and $\overline{g}$ are the average SNRs of the main and eavesdropper channels respectively. In this

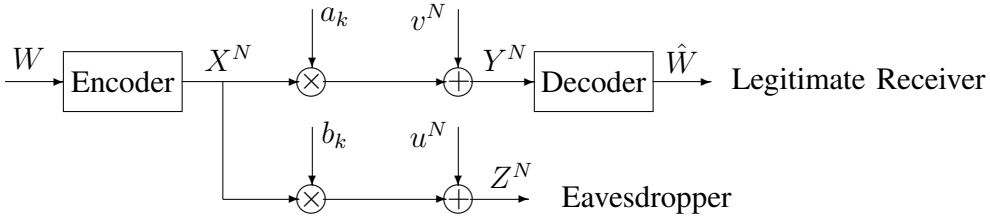

Figure 1. System model

case we can show that the cumulative density functions of $C^{\mathcal{D}}$ and $C^{\mathcal{E}}$ are

$$F_{C^{\mathcal{D}}}(x) = 1 - e^{-\frac{2^{2x}-1}{\bar{h}}} \tag{3}$$

$$F_{C^{\mathcal{E}}}(x) = 1 - e^{-\frac{2^{2x}-1}{\bar{g}}} \tag{4}$$

and $p_{C^{\mathcal{D}}}$ and $p_{C^{\mathcal{E}}}$ can be written as

$$p_{C^{\mathcal{D}}}(x) = 2 \cdot \log(2) \cdot p_H(2^{2x} - 1) \cdot 2^{2x} \tag{5}$$

$$p_{C^{\mathcal{E}}}(x) = 2 \cdot \log(2) \cdot p_G(2^{2x} - 1) \cdot 2^{2x} \tag{6}$$

B. Wyner codes

In this subsection, we consider a single block transmission (i.e. $K = 1$) and introduce Wyner codes. In [2] Wyner introduced the notion of a wiretap channel. It is the most basic channel model that takes security constraint into account. In a wiretap channel, the source wishes to convey a message $w \in \mathcal{W}$, which is chosen uniformly at random from the message set $\mathcal{W}$, to the legitimate receiver through the main channel. The sender performs this task by encoding w as a vector x^N of length N and transmitting x^N. Let $C(N, R_0, R_s)$ denote a Wyner code to transmit the confidential message set $\mathcal{W} = \{1, 2, .., 2^{NR_s}\}$ where N is the codeword length, R_0 is the main channel code rate and R_s ($R_s \leq R_0$) is the secrecy information rate. The basic idea of Wyner codes is to use a stochastic encoder to increase the secrecy level [2]. The Wyner code is constructed based on random binning [2] as follows. We generate 2^{NR_0} codewords $x^N(w, v)$, where $w = 1, 2, .., 2^{NR_s}$ and $v = 1, 2, .., 2^{N(R_0-R_s)}$, by choosing the $N2^{NR_0}$ symbols $x_i(w, v)$ independently at random according to the input distribution $p(x)$. To encode the message $w \in \mathcal{W}$, we uniformly at random select v from $\{1, 2, .., 2^{N(R_0-R_s)}\}$ and transmit $x^N = x^N(w, v)$.

Assume that the transmitted signals are received at the legitimate receiver and the eavesdropper via channel SNRs h and g respectively. Let $P_e(h)$ be the average decoding error probability for the legitimate receiver:

$$P_e(h) = \sum_{w \in \mathcal{W}} \Pr\{\hat{w} \neq w | w \text{ sent}, h\} \Pr(w) \tag{7}$$

where $\hat{w}$ is the the output of the legitimate decoder after observing y^N given that the message w is sent.

To measure the amount of information that the eavesdropper receives about W we use the following normalized conditional entropy $H(W|g, z^N)/N$ which we call the equivocation rate. We want the equivocation rate to be as high as possible, and ideally it should equal the rate R_s. Thus *perfect secrecy* is achieved if for all $\epsilon > 0$ the equivocation rate satisfies:

$$\frac{H(W|g, z^N)}{N} \geq \frac{H(W)}{N} - \epsilon \tag{8}$$

We recall now the definition 1 in [4] about *good* code. A code C of length N is good for a wiretap channel with the channel SNRs pair (h, g) if $P_e(h) \leq \epsilon$ (reliability condition) and the perfect secrecy requirement (8) can be achieved (security condition) for all $\epsilon > 0$ and sufficiently large N. Wyner shows that the achievable rates pair (R_0, R_s) for a good code satisfy:

$$R_0 \leq I(X; Y) \tag{9}$$

$$R_0 - R_s \geq I(X; Z) \tag{10}$$

We use the notations $N_s = N \cdot R_s$ to denote the number of secure bits (information bits) and $N_0 = N \cdot R_0$. The rate $R' = R_0 - R_s$ is the rate sacrificed to provide secrecy.

The codebook of the channel code is revealed to all nodes. We assume random coding with long codewords lengths may be used and the receivers implement the typical-set decoding which allow us to find the performance limits for any practical scheme.

III. SECURE HARQ PROTOCOLS

We consider incremental redundancy secure HARQ as a transmission protocol. The N-symbols of the codeword are divided into K sub-codewords $\mathbf{x_k}$, $k = 1, .., K$ each of length N_k where $N = \sum_{k=1}^{K} N_k$. The ARQ process starts by sending the first sub-codeword $\mathbf{x}_1$ under the channel SNRs pair (h_1, g_1). Decoding of this code is performed at the intended receiver, while the secrecy

level is measured at the eavesdropper. If a second retransmission is requested by the receiver due to unsuccessful decoding, the second sub-codeword $\mathbf{x}_2$ is sent under possibly different channel conditions (h_2, g_2). Now decoding and equivocation calculation are attempted at the receiver and eavesdropper by combining the previous block $\mathbf{x}_1$ with the new block $\mathbf{x}_2$. This continues until the maximum number of transmissions attempts K is reached or until the successful decoding of the message at the legitimate receiver.

A. Incremental redundancy scheme [4]

In the system model of [4], two protocols are considered: repetition time diversity and incremental redundancy. We will be interested here by the incremental redundancy scheme. The transmitter obtains a 1-bit ACK/NACK feedback from the legitimate receiver to declare a successful/unsuccessful decoding via an error free public channel. The incremental redundancy protocol is considered when the K sub-codewords $\mathbf{x_k}$ have the same length, i.e. $N_1 = N_2 = .. = N_K = \lfloor \frac{N}{K} \rfloor$ and N is multiple of K. Similarly to the case of a single block transmission, the authors study the error performance and the secrecy level after k transmissions, $k = 1, .., K$. Let $\mathbf{x}(k) = [\mathbf{x}_1, .., \mathbf{x}_k]$, $\mathbf{y}(k) = [\mathbf{y}_1, .., \mathbf{y}_k]$ and $\mathbf{z}(k) = [\mathbf{z}_1, .., \mathbf{z}_k]$ denote the input, the output at the legitimate receiver and the output at the eavesdropper after k transmissions respectively. For a given channel SNRs vectors pairs (**h**, **g**), the average error probability after the kth transmission is defined as:

$$P_e(k|\mathbf{h}) = \sum_{w \in \mathcal{W}} \Pr\{\hat{w} \neq w | w \text{ sent}, \mathbf{h}\} \Pr(w) \tag{11}$$

where $\hat{w}$ denotes the output of the legitimate decoder after k transmissions. We say that perfect secrecy is achieved after k transmissions if for all $\epsilon > 0$ the equivocation rate satisfies:

$$\frac{H(W|\mathbf{g}, \mathbf{z}^N)}{kN_1} \geq \frac{H(W)}{kN_1} - \epsilon \tag{12}$$

where $N_1 = \lfloor \frac{N}{K} \rfloor$ and the term in the left side of the inequality is the secrecy level after k transmissions.

A code C of length mN_1 is called a *good* code in [4] for the k-block transmission and a channel SNRs vectors pairs (**h**, **g**) if $P_e(k|\mathbf{h}) \leq \epsilon$ and the perfect secrecy requirement (12) can be achieved for all $\epsilon > 0$ and sufficiently large N.

Since the transmitter does not have any information on the instantaneous channel state (except channel statistics); that is, one cannot choose the code rate pair based on a particular fading

channel state. Instead, an in-advance fixed (Wyner) code rate pair is used for all channel conditions. In [4] the authors describe a secure channel set and demonstrate that there exists a Wyner code sequence good for all channel pairs in this set. Then, they evaluate the performance of the INR protocol when the codewords of the mother Wyner code are transmitted in at most K transmissions during the secure HARQ session using the equivalent parallel channel model. In the following, we recall the theorem 1 in [4]:

Theorem 1: Consider the secure INR protocol based on compatible Wyner codes $\{C_K, C_{K-1}, .., C_1\}$ where $C_m \in \mathcal{C}(\frac{KR_0}{k}, \frac{KR_s}{k}, kN_1)$, $k = 1, .., K$

For a given pair of rates (R_0, R_s) and a fixed input distribution $p(x)$, let $\mathcal{P}(k)$ denote the union of all channel SNRs vectors pairs (**h**, **g**) satisfying

$$R_0 \leq \frac{1}{K} \sum_{i=1}^{k} I(X; Y|h_i) \tag{13}$$

$$R_0 - R_s \geq \frac{1}{K} \sum_{i=1}^{k} I(X; Z|g_i) \tag{14}$$

Then there exists a family of rate compatible Wyner codes $\{C_K, C_{K-1}, .., C_1\}$ such that C_k is good for all channel SNRs vectors pairs (**h**, **g**) $\in \mathcal{P}(k)$ for $k = 1, .., K$. $\square$

The outage events are also defined in [4] when the channel SNRs vector pair does not belong to the secure channel set. The connection outage event is considered when the main channel to the legitimate receiver cannot support the codeword rate R_0. Then the message will not be correctly decoded by the legitimate receiver. The secrecy outage happens when the eavesdropper channel can support a rate greater than the redundancy rate $R' = R_0 - R_s$.

The problem of maximizing the achievable secrecy throughput η under connection outage (f_0) and secrecy outage (f_s) constraints was investigated. The secrecy throughput η is defined to be the average number of bits decoded at the legitimate receiver. It can be written according to the renewal-reward [1],[8] theorem as $\eta(R_0, R_s) = \frac{KR_s \cdot (1-f_0)}{\mathbb{E}[\mathcal{K}]}$. Then the maximization problem is shown in [4] as :

$$\max_{R_0, R_s} \quad \eta(R_0, R_s)$$
$$s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases}$$

where ξ_ϵ and ξ_s are the target outage probabilities and $\mathcal{K}$ is a random variable representing the number of transmission in an HARQ session.

B. Adaptive incremental redundancy scheme

In this paper, we consider a general system model where the transmitter uses multi-level feedback channels from the both the legitimate receiver and the eavesdropper, which are assumed error free. Moreover, we consider that the sub-codewords $\mathbf{x_k}$ may not have the same length.

The coding scheme we described is revealed to all receivers. After k transmissions, each receiver applies the maximum likelihood decoding using the channel observations obtained up to the kth transmission. The condition of successful decoding at the legitimate receiver after k transmissions is that the average accumulated mutual information is larger than the overall transmission rate. This condition was written for equally length subcodeword in (13). In our system model where the sub-codewords $\mathbf{x_k}$ may not have the same length, this condition is written as:

$$\frac{\sum_{l=1}^{k} C_l^{\mathcal{D}} \cdot N_l}{\sum_{l=1}^{k} N_l} \geq \frac{N_0}{\sum_{l=1}^{k} N_l} \tag{15}$$

where N_l is the duration of the sub-codeword sent at lth transmission and $C_l^{\mathcal{D}} = I(X;Y|h_l) = \frac{1}{2}\log_2(1+h_l)$. For convenience, we normalize the values of N_l using $\rho_l = \frac{N_l}{N_0}$ which is interpreted as a redundancy measured by the number of channel uses per information bit. It might be noticed that the redundancy ρ_k is equal to the inverse of the kth transmission rate. Since the rate of the transmission attempts are not the same, we talk about variable rate transmission. Now (15) can be written as follows:

$$I_k^{\mathcal{D}} \stackrel{\triangle}{=} \sum_{l=1}^{k} C_l^{\mathcal{D}} \cdot \rho_l \geq 1 \tag{16}$$

We call $I_k^{\mathcal{D}}$ the " state of the decoder" at the legitimate receiver (D).

The condition for secrecy at the eavesdropper after k transmissions is that the average accumulated mutual information is less than the difference between the transmission rate (main channel code rate) and the secrecy information rate:

$$\frac{\sum_{l=1}^{k} C_l^{\mathcal{E}} \cdot N_l}{\sum_{l=1}^{k} N_l} \leq \frac{N_0 - N_s}{\sum_{l=1}^{k} N_l}$$

equivalently,

$$I_k^{\mathcal{E}} \stackrel{\triangle}{=} \sum_{l=1}^{k} C_l^{\mathcal{E}} \cdot \rho_l + \gamma \leq 1 \tag{17}$$

where $C_l^{\mathcal{E}} = I(X;Z|g_l) = \frac{1}{2}\log_2(1+g_l)$ and $\gamma = \frac{R_s}{R_0} = \frac{N_s}{N_0} = \frac{N_s}{N_s+N'}$. N', which is the number of additional bits to ensure secrecy at eavesdropper, is not fixed apriori at the transmitter. In

this paper, we study the case where the transmitter uses the same γ (or N') for all channel realizations ($\gamma_k = \gamma \ \forall k \in \{1, .., K\}$). We call $I_k^{\mathcal{E}}$ the state of the decoder at the eavesdropper E (in fact, it is the sum of the state at the eavesdropper decoder and the parameter γ).

From (16) and (17) we know that the decoding error events in the k-th transmission at the legitimate receiver and the eavesdropper depend on $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ which can be communicated to the sender via the multilevel feedback and on $C_k^{\mathcal{D}}$ and $C_k^{\mathcal{E}}$ which are unknown at the transmitter. Consequently, $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ are the only parameters required to adapt the redundancy ρ_k via a scalar function.

We consider the following policy for the transmission attempt k:

$$\rho_k = \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}), \quad k = 2, ..., K$$

where

$$\rho_k = \begin{cases} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) & \text{if } I_{k-1}^{\mathcal{D}} < 1 \ \text{ and } I_{k-1}^{\mathcal{E}} < 1 \\ \rho_k(I_{k-1}^{\mathcal{D}}) & \text{if } I_{k-1}^{\mathcal{D}} < 1 \ \text{ and } I_{k-1}^{\mathcal{E}} \geq 1 \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

This makes our work different from [4] which consider the special case where $\rho_k = \rho \ \forall k$. The goal now is to find the rate adaptation policies and γ that solve the constrained secrecy throughput maximization problem.

IV. Problem Formulation

Our objective in this paper is to maximize the achievable secrecy throughput of the system under investigation. The secrecy throughput is a relevant performance criterion as it can be directly related to the channel secrecy capacity. Based on the reward-renewal theorem [1],[8], the secrecy throughput is defined by the ratio between the number of information bits received reliably N_s^* and the expected number of channel uses $\overline{N}$ required by the HARQ protocol to deliver the packet in up to K transmission attempts:

$$\eta = \frac{N_s^*}{\overline{N}}$$

Since the transmitter has no instantaneous channel information, the rate can be adapted to instantaneous channel conditions. Instead, we consider the outage performance of secure HARQ

protocols. Hence, we consider that the service quality is acceptable as long as the percentage of information bits not successfully decoded by the legitimate receiver is less than ξ_e and the percentage of information bits successfully decoded by the eavesdropper is less than ξ_s. Thus, we define the connection outage probability f_0 by the probability of decoding failure after K transmissions at the legitimate receiver and the secrecy outage probability f_s by the probability of a successful decoding at the eavesdropper in the last transmission. The outage probabilities are used to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link.

- $N_s^* = N_s \cdot (1 - f_0)$, and f_0 can be written as:

$$f_0 = \Pr\{I_K^{\mathcal{D}} < 1\} = \mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}}\{\mathbb{I}(I_K^{\mathcal{D}} < 1)\} = \int_0^1 dx \int_\gamma^\infty dy \; p_{I_K^{\mathcal{D}} \; I_K^{\mathcal{E}}}(x, y) \tag{19}$$

  where $\mathbb{I}(x) = 1$ if x is true and $\mathbb{I}(x) = 0$ if x is false. $p_{I_K^{\mathcal{D}} \; I_K^{\mathcal{E}}}(x, y)$ is the joint pdf of $I_K^{\mathcal{D}}$ and $I_K^{\mathcal{E}}$.

- The expected number of channel uses is given by $\overline{N} = \sum_{k=1}^K \overline{N}_k$, where $\overline{N}_k$ is the expected number of channel uses in the kth transmission attempt:

$$\overline{N}_k = N_0 \cdot \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}}\{\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})\} = N_0 \cdot \int_0^1 dx \int_\gamma^\infty dy \; \rho_k(x, y) \cdot p_{I_{k-1}^{\mathcal{D}} \; I_{k-1}^{\mathcal{E}}}(x, y)$$

Thus the secrecy throughput is

$$\eta = \gamma \cdot \frac{1 - f_0}{\sum_{k=1}^K \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}}\{\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})\}} \tag{20}$$

Let $\mathcal{K}$ denotes the number of transmission in an HARQ session (the index of the last transmissions). The secrecy outage probability f_s can be expressed as:

$$\begin{aligned} f_s &= \Pr(I_{\mathcal{K}}^{\mathcal{E}} \geq 1) \\ &= \sum_{k=1}^K \Pr(I_{\mathcal{K}}^{\mathcal{E}} \geq 1, \mathcal{K} = k) \\ &= \sum_{k=1}^K \Pr(\mathcal{K} = k) \cdot \Pr(I_{\mathcal{K}}^{\mathcal{E}} \geq 1 | \mathcal{K} = k) \\ &= \sum_{k=1}^K \Pr(\mathcal{K} = k) \cdot \Pr(I_k^{\mathcal{E}} \geq 1) \end{aligned} \tag{21}$$

where:

- The probability mass function of $\mathcal{K}$ can be expressed as:

$$\begin{aligned}\Pr(\mathcal{K}=k) &= \Pr(I_{k-1}^{\mathcal{D}}<1, I_k^{\mathcal{D}}\geq 1)\\ &= \Pr(I_{k-1}^{\mathcal{D}}<1) - \Pr(I_{k-1}^{\mathcal{D}}<1, I_k^{\mathcal{D}}<1)\\ &= \Pr(I_{k-1}^{\mathcal{D}}<1) - \Pr(I_k^{\mathcal{D}}<1)\\ &= \mathbb{E}_{C_1^{\mathcal{D}},..,C_{k-1}^{\mathcal{D}}}\{\mathbb{I}(I_{k-1}^{\mathcal{D}}<1)\} - \mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}}\{\mathbb{I}(I_k^{\mathcal{D}}<1)\}\end{aligned}$$

  for $k<K$ and

$$\Pr(\mathcal{K}=K) = \Pr(I_{K-1}^{\mathcal{D}}<1) = \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}}\{\mathbb{I}(I_{K-1}^{\mathcal{D}}<1)\}$$

- The probability that the eavesdropper can decode the confidential message at the kth transmission is:

$$\Pr(I_k^{\mathcal{E}}\geq 1) = \mathbb{E}_{C_1^{\mathcal{E}},..,C_k^{\mathcal{E}}}\{\mathbb{I}(I_k^{\mathcal{E}}\geq 1)\} = \int_0^{\infty} dx \int_1^{\infty} dy\ p_{I_k^{\mathcal{D}}\ I_k^{\mathcal{E}}}(x,y)$$

The secrecy throughput in (20) depends on the model of the channel and on the coding and decoding scheme. Here, we assume that the coding and decoding scheme is capacity-achieving as in [1] and we provide the performance limits for any practical scheme. The secrecy throughput optimization problem under outages constraints is written as:

$$\begin{aligned}&\max_{\gamma,\rho_1,...,\rho_K} \quad \eta(\rho_1,...,\rho_K,\gamma)\\ &s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases}\end{aligned} \tag{22}$$

where ξ_ϵ and ξ_s are the target outage probabilities.

V. Constrained secrecy throughput optimization using dynamic programming

The design of the adaptive incremental redundancy HARQ scheme consists in finding the rate adaptation policies ρ_k, $k=1,...,K$ and γ which maximize the secrecy throughput under outage probabilities constraints. Based on channel statistics, we can obtain the code parameters to achieve the maximum secrecy throughput while satisfying the outage constraints.

Obviously, the solution of the multidimensional problem (22) is too difficult to find using exhaustive search method. To solve this problem we use exhaustive search to find the optimal γ which maximize the throughput. Thus, we solved problem (22) for different values of $\gamma\in[0,1]$.

Once $\gamma \in [0,1]$ is fixed, we maximize the secrecy throughput subject to ρ_k. The optimization problem can now be written as

$$\max_{\rho_1,...,\rho_K} \quad \eta(\rho_1,...,\rho_K;\gamma)$$

$$s.t. \begin{cases} f_0 & \leq \xi_\epsilon \\ f_s & \leq \xi_s \end{cases} \tag{23}$$

We will describe later how to make the choice of γ in the simulations. Now suppose that γ is fixed for an arbitrary value in $[0,1]$. Next, we explain how to solve (23) using "dynamic programming".In order to maximize the secrecy throughput η in (23), we define an auxiliary optimization problem:

$$U(\xi_\epsilon,\xi_s) = \min_{\rho_1,...,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I^{\mathcal{D}}_{k-1},I^{\mathcal{E}}_{k-1}} \left\{ \rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) \right\} \quad \text{s.t.} \quad f_0 = \xi_\epsilon \quad \text{and} \quad f_s = \xi_s \tag{24}$$

The maximal secrecy throughput is obtained solving

$$\hat{\eta} = \max_{\xi_\epsilon,\xi_s} \frac{1-\xi_\epsilon}{U(\xi_\epsilon,\xi_s)} = \frac{1-\hat{\xi}_\epsilon}{U(\hat{\xi}_\epsilon,\hat{\xi}_s)} \tag{25}$$

and the secrecy throughput maximization under outage constraints $\hat{\eta}_{\epsilon s}$

$$\hat{\eta}_{\epsilon s} = \max_{\rho_1,...,\rho_K} \ \eta, \quad \text{s.t.} \ \ f_0 \leq \xi_\epsilon \quad \text{and} \quad f_s \leq \xi_s$$

is obtained as

$$\hat{\eta}_{\epsilon s} = \begin{cases} \hat{\eta} & \text{if } \hat{\xi}_\epsilon < \xi_\epsilon \quad \text{and } \hat{\xi}_s < \xi_s \\ \\ \gamma \cdot \frac{1-\xi_\epsilon}{U(\xi_\epsilon,\xi_s)} & \text{otherwise.} \end{cases}$$

Thus the design of adaptation policies requires solving (24) which can be done using Lagrangian multipliers λ_1 and λ_2:

$$U(\xi_\epsilon,\xi_s) = \min_{\rho_1,...,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I^{\mathcal{D}}_{k-1},I^{\mathcal{E}}_{k-1}} \left\{ \rho_k(I^{\mathcal{D}}_{k-1}, I^{\mathcal{E}}_{k-1}) \right\} + \lambda_1 \cdot (f_0 - \xi_\epsilon) + \lambda_2 \cdot (f_s - \xi_s)$$

$$\text{s.t.} \ \ \lambda_1 \cdot (f_0 - \xi_\epsilon) = 0 \quad \text{and} \ \ \lambda_2 \cdot (f_s - \xi_s) = 0 \tag{26}$$

We are interested in evaluating $U(\xi_\epsilon,\xi_s)$ for many values of ξ_ϵ and ξ_s. Since for each couple of λ_1 and λ_2 corresponds a connection outage f_0 and a secrecy outage f_s, we can solve (26) for

Step 0	$\lambda_1 \leftarrow \lambda_1^{(0)}$, $\lambda_2 \leftarrow \lambda_2^{(0)}$
Step ℓ	1. solve $J^{\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)}}$ in (28) using Table II: $J^{\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)}} = J(\lambda_1^{(\ell-1)}, \lambda_2^{(\ell-1)}, \gamma, \overline{h}, \overline{g})$ 2. calculate the joint probabilities function in (39) and (40) for $k = 1, .., K$ 3. calculate the outage $f_0^{(\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)})}$ using (19). 4. update λ_1: $\lambda_1^{(\ell)} = [\lambda_1^{(\ell-1)} + \beta(f_0^{(\lambda_1^{(\ell-1)},\lambda_2^{(\ell-1)})} - \xi_0)]^+$ where $[.]^+ = \max(., 0)$
	1. solve $J^{\lambda_1^{(\ell)},\lambda_2^{(\ell-1)}}$ in (28) using Table II: $J^{\lambda_1^{(\ell)},\lambda_2^{(\ell-1)}} = J(\lambda_1^{(\ell)}, \lambda_2^{(\ell-1)}, \gamma, \overline{h}, \overline{g})$ 2. calculate the joint probabilities function in (39) and (40) for $k = 1, .., K$ 3. calculate the outage $f_s^{(\lambda_1^{(\ell)},\lambda_2^{(\ell-1)})}$ using (21). 4. update λ_2: $\lambda_2^{(\ell)} = [\lambda_2^{(\ell-1)} + \beta(f_s^{(\lambda_1^{(\ell)},\lambda_2^{(\ell-1)})} - \xi_s)]^+$ where $[.]^+ = \max(., 0)$
Stopping criterion	$\frac{1}{\beta}\lvert\lambda_1^{(\ell)} - \lambda_1^{(\ell-1)}\rvert \leq \epsilon_1$ $\frac{1}{\beta}\lvert\lambda_2^{(\ell)} - \lambda_2^{(\ell-1)}\rvert \leq \epsilon_2$

Table I

NUMERICAL SOLUTION FOR SOLVING (23) FOR A FIXED $\gamma \in [0, 1]$ WHERE $\overline{h}$ AND $\overline{g}$ ARE THE AVERAGE SNRS OF THE MAIN CHANNEL AND EAVESDROPPER CHANNEL RESPECTIVELY.

different λ_1 and λ_2. Thus, to solve (20) we employ auxiliaries weighting multipliers λ_1 and λ_2 and try to minimize the denominator of (20), f_0 and f_s at the same time as:

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,...,\rho_K} \sum_{k=1}^{K} \mathbb{E}_{I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}} \left\{ \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \right\} + \lambda_1 \cdot f_0(\rho_1, ..., \rho_K) + \lambda_2 \cdot f_s(\rho_1, ..., \rho_K) \quad (27)$$

and next use $J^{\lambda_1,\lambda_2} = U(f_0(\rho_1, ..., \rho_K))$.

Since $I_{k-1}^{\mathcal{D}}$ and $I_{k-1}^{\mathcal{E}}$ depend on $C_1^{\mathcal{D}}, .., C_{k-1}^{\mathcal{D}}$ and $C_1^{\mathcal{E}}, .., C_{k-1}^{\mathcal{E}}$ respectively, we can write:

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,...,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}, C_1^{\mathcal{E}},..,C_{K-1}^{\mathcal{E}}} \sum_{k=1}^{K} \left\{ \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \right\} + \lambda_1 \cdot f_0 + \lambda_2 \cdot f_s \quad (28)$$

Where for simplicity of notation we write $f_0(\rho_1, ..., \rho_K) = f_0$ and $f_s(\rho_1, ..., \rho_K) = f_s$.

In this work, we use the iterative algorithm proposed in Table I in order to vary λ_1 and λ_2. We use gradient-search method to optimize alternately λ_1 and λ_2: in the first step, we update λ_2 using gradient algorithm and in the next step we fix λ_2 and we update λ_1.

Now **assume that λ_1 and λ_2 are fixed**. The goal is to solve (28) using these fixed values of λ_1 and λ_2. First we can observe that the states of decoders of legitimate receiver and eavesdropper

at time k can be written in function of the previous state as follows

$$I_k^{\mathcal{D}} = I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k$$

where $I_0^{\mathcal{D}} = 0$, and

$$I_k^{\mathcal{E}} = I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k$$

where $I_0^{\mathcal{E}} = \gamma$.

Now we can write (28) in the recursive form using (19) and (21):

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,\ldots,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}},C_1^{\mathcal{E}},..,C_{K-1}^{\mathcal{E}}} \left\{ \sum_{k=1}^{K} \rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) \right\} + \lambda_1 \cdot \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_K^{\mathcal{D}}} \left\{ \mathbb{I}(I_K^{\mathcal{D}} < 1) \right\} \right]$$

$$+\lambda_2 \cdot \sum_{k=1}^{K-1} \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_k^{\mathcal{D}}} \left\{ \mathbb{I}(I_{k-1}^{\mathcal{D}} < 1) - \mathbb{I}(I_k^{\mathcal{D}} < 1) \right\} \cdot \mathbb{E}_{C_1^{\mathcal{E}},..,C_k^{\mathcal{E}}} \left\{ \mathbb{I}(I_k^{\mathcal{E}} \geq 1) \right\} \right]$$

$$+\lambda_2 \cdot \left[\mathbb{E}_{C_1^{\mathcal{D}},..,C_{K-1}^{\mathcal{D}}} \left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \mathbb{E}_{C_1^{\mathcal{E}},..,C_K^{\mathcal{E}}} \left\{ \mathbb{I}(I_K^{\mathcal{E}} \geq 1) \right\} \right]$$

Due to the independence of channels, we can write $\mathbb{E}_{C_k^{\mathcal{D}}} \left\{ f_1(C_k^{\mathcal{D}}) \right\} \cdot \mathbb{E}_{C_k^{\mathcal{E}}} \left\{ f_2(C_k^{\mathcal{E}}) \right\} = \mathbb{E}_{C_k^{\mathcal{D}},C_k^{\mathcal{E}}} \left\{ f_1(C_k^{\mathcal{D}}) \cdot f_2(C_k^{\mathcal{E}}) \right\}$, therefore:

$$J^{\lambda_1,\lambda_2} = \min_{\rho_1,\ldots,\rho_K} \mathbb{E}_{C_1^{\mathcal{D}},C_1^{\mathcal{E}}} \left\{ \rho_1 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_0^{\mathcal{D}} < 1) - \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1 < 1) \right\} \cdot \left\{ \mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1 \geq 1) \right\} \right] \right.$$

$$+\mathbb{E}_{C_2^{\mathcal{D}},C_2^{\mathcal{E}}} \left\{ \rho_2 + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_1^{\mathcal{D}} < 1) - \mathbb{I}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2 < 1) \right\} \cdot \left\{ \mathbb{I}(I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 \geq 1) \right\} \right] \right.$$

$$+....$$

$$\left. \left. +\mathbb{E}_{C_K^{\mathcal{D}},C_K^{\mathcal{E}}} \left\{ \rho_K + \lambda_1 \cdot \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1) + \lambda_2 \cdot \left[\left\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \right\} \cdot \left\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K \geq 1) \right\} \right] \right. \right\} ... \right\} \right\}$$

We observe that the initial complicated problem can be simplified by breaking it into simpler subproblems in a recursive manner. Consequently the dynamic programming method is applicable to perform the optimization. Then J^{λ_1,λ_2} can be written via dynamic programming recursion:

$$J^{\lambda_1,\lambda_2} = J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}})$$

$$J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}}) = \min_{\rho_1} \mathbb{E}_{C_1^{\mathcal{D}}, C_1^{\mathcal{E}}} \Bigg\{ \rho_1 + \lambda_2 \cdot \Bigg[\Bigg\{ \mathbb{I}(I_0^{\mathcal{D}} < 1) - \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1 < 1) \Bigg\} \cdot \Bigg\{ \mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1 \geq 1) \Bigg\} \Bigg] + J_2^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1, I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1) \Bigg\}$$

$$J_2^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}) = \min_{\rho_2} \mathbb{E}_{C_2^{\mathcal{D}}, C_2^{\mathcal{E}}} \Bigg\{ \rho_2 + \lambda_2 \cdot \Bigg[\Bigg\{ \mathbb{I}(I_1^{\mathcal{D}} < 1) - \mathbb{I}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2 < 1) \Bigg\} \cdot \Bigg\{ \mathbb{I}(I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 \geq 1) \Bigg\} \Bigg] + J_3^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2, I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2) \Bigg\}$$

...

$$J_K^{\lambda_1,\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} \mathbb{E}_{C_K^{\mathcal{D}}, C_K^{\mathcal{E}}} \Bigg\{ \rho_K + \lambda_2 \cdot \Bigg[\Bigg\{ \mathbb{I}(I_{K-1}^{\mathcal{D}} < 1) \Bigg\} \cdot \Bigg\{ \mathbb{I}(I_{K-1}^{\mathcal{E}} + C_K^{\mathcal{E}} \cdot \rho_K \geq 1) \Bigg\} \Bigg] + \lambda_1 \cdot \mathbb{I}(I_{K-1}^{\mathcal{D}} + C_K^{\mathcal{D}} \cdot \rho_K < 1)$$

Now, to solve the problem for given λ_1 and λ_2, we start from the last equation $J_K^{\lambda_1,\lambda_2}$, where we should obtain the value of ρ_K that minimize $J_K^{\lambda_1,\lambda_2}$ for each values of $I_{K-1}^{\mathcal{D}}$ and $I_{K-1}^{\mathcal{E}}$, which have to be discretized to L_1 and L_2 points over the interval [0,1) and [γ,1] respectively. The problem should be solved starting from step K and going recursively up to $k = 1$ to find all the optimum policies ρ_k for given λ_1 and λ_2. Thus, the global optimization of the possibly non-convex function $J^{\lambda_1\lambda_2}$ is reduced to $(K-1) \cdot L_1 \cdot L_2 + 1$ one dimensional optimization problems which is a noticeable reduction in complexity of the problem.

$J_k^{\lambda_1,\lambda_2}$ $(k < K)$ and $J_K^{\lambda_1,\lambda_2}$ can be also expressed as

$$J_K^{\lambda_1,\lambda_2}(I_{K-1}^{\mathcal{D}}, I_{K-1}^{\mathcal{E}}) = \min_{\rho_K} \ \rho_K + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_{K-1}^{\mathcal{E}}}{\rho_K} \right) \right\} \right] + \lambda_1 \cdot F_{C^{\mathcal{D}}} \left(\frac{1 - I_{K-1}^{\mathcal{D}}}{\rho_K} \right) \quad (29)$$

$$J_k^{\lambda_1,\lambda_2}(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}}) = \min_{\rho_k} \ \rho_k + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{D}}} \left(\frac{1 - I_{k-1}^{\mathcal{D}}}{\rho_k} \right) \right\} \cdot \left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_{k-1}^{\mathcal{E}}}{\rho_k} \right) \right\} \right] + \mathbb{E}_{C_k^{\mathcal{D}}, C_k^{\mathcal{E}}} \left\{ J_{k+1}^{\lambda_1,\lambda_2}(I_{k-1}^{\mathcal{D}} + C_k^{\mathcal{D}} \cdot \rho_k, I_{k-1}^{\mathcal{E}} + C_k^{\mathcal{E}} \cdot \rho_k) \right\} \quad (30)$$

where $F_{C^{\mathcal{D}}}$ and $F_{C^{\mathcal{E}}}$ are the cumulative density functions of $C^{\mathcal{D}}$ and $C^{\mathcal{E}}$ respectively.

$J(\lambda_1, \lambda_2, \gamma, \overline{h}, \overline{g})$: Let $I^D = 0 \rightarrow 1$ a vector of L_1 points between 0 and 1. Let $I^E = \gamma \rightarrow 1$ a vector of L_2 points between γ and 1	
for $k = K : -1 : 1$	for each k we want to obtain the optimal $\rho_k(I^D, I^E)$ by solving (30) or (29) depending on k: if $k = 1$ (i.e. in this case we solve (34).) initialize $\rho_k \leftarrow 1 \times 1$ matrix and $J_k \leftarrow 1 \times 1$ matrix set $i_0^D = 0$ and $i_0^E = \gamma$, in this case we need only to know two values: $\rho_1(0, \gamma)$ and $J_1(0, \gamma)$ $[\rho_k \ J_k]$=min_$J_k(J_{k+1}, \lambda_2, \overline{h}, \overline{g}, i_0^D, i_0^E, \gamma)$ this function is explained in Table III else initialize $\rho_k \leftarrow L_1 \times L_2$ matrix and $J_k \leftarrow L_1 \times L_2$ matrix for $i^D = I^D$ (i.e. i^D is a value between 0 and 1) for $i^E = I^E$ (i.e. i^E is a value between γ and 1) for each couple (i^D, i^E) we need to optimize $\rho_k(i^D, i^E)$ and $J_k(i^D, i^E)$ using (30) or (29) if $k < K$ (solving (30).) $\big[\rho_k(i^D, i^E) \ J_k(i^D, i^E)\big]$=min_$J_k\big(J_{k+1}, \lambda_2, \overline{h}, \overline{g}, i^D, i^E, \gamma\big)$ this function is explained in Table III elseif $k = K$ (solving (29).) $\big[\rho_k(i^D, i^E) \ J_k(i^D, i^E)\big]$=min_$J_K\big(\lambda_1, \lambda_2, \overline{h}, \overline{g}, i^D, i^E, \gamma\big)$ this function is explained in Table IV end end end end save ρ_k and J_k
end	

Table II

ALGORITHM USED FOR SOLVING (28). THE FUNCTION $J(\lambda_1, \lambda_2, \gamma, \overline{h}, \overline{g})$ SOLVES J^{λ_1, λ_2} IN (28). IT TAKES AS PARAMETERS THE LAGRANGIAN MULTIPLIERS λ_1 AND λ_2, γ AND THE AVERAGE SNRS OF THE MAIN CHANNEL AND EAVESDROPPER CHANNEL RESPECTIVELY $\overline{h}$ AND $\overline{g}$.

1) Example with 3 transmissions ($K = 3$): Let study the case where $K = 3$, the dynamic programming recursion can be written as:

$$J^{\lambda_1, \lambda_2} = J_1^{\lambda_1, \lambda_2}(I_0^{\mathcal{D}}, I_0^{\mathcal{E}})$$

The function min_$J_k\left(J_{k+1},\lambda_2,\overline{h},\overline{g},i^D,i^E,\gamma\right)$ solves (30) where $I^{\mathcal{D}}_{k-1}=i^D$ and $I^{\mathcal{E}}_{k-1}=i^E$

and J_{k+1} is a $L_1\times L_2$ matrix:

$\left[\rho_k^{(i^D,i^E)}\ \ J_k^{(i^D,i^E)}\right]$=min_$J_k\left(J_{k+1},\lambda_2,\overline{h},\overline{g},i^D,i^E,\gamma\right)$

for $\rho=0:0.01:\rho^{max}$ (ρ^{max} is arbitrary fixed during simulations)

calculate $f(\rho)=\rho+\lambda_2\cdot\left[\left\{1-F_{C^{\mathcal{D}}}\left(\frac{1-i^D}{\rho}\right)\right\}\cdot\left\{1-F_{C^{\mathcal{E}}}\left(\frac{1-i^E}{\rho}\right)\right\}\right]+\mathbb{E}_{C_k^{\mathcal{D}},C_k^{\mathcal{E}}}\left\{J_{k+1}(i^D+C_k^{\mathcal{D}}\cdot\rho,i^E+C_k^{\mathcal{E}}\cdot\rho)\right\}$

using the approximation in (38) to evaluate the expectation. Having the matrix J_{k+1} as function parameter,

we can know the value of $J_{k+1}(i^D+C_k^{\mathcal{D}}\cdot\rho,i^E+C_k^{\mathcal{E}}\cdot\rho)$ for each ρ and for a fixed values x and y of $C_k^{\mathcal{D}}$ and $C_k^{\mathcal{E}}$ resp.:

$\mathbb{E}_{C_k^{\mathcal{D}},C_k^{\mathcal{E}}}\left\{J_{k+1}(i^D+C_k^{\mathcal{D}}\cdot\rho,i^E+C_k^{\mathcal{E}}\cdot\rho)\right\}=\sum_{x=0}^{x^{\max}}\sum_{y=0}^{y^{\max}}J_{k+1}\left(i^D+x\cdot\rho,i^E+y\cdot\rho\right)\cdot p_{C^{\mathcal{D}}}(x)\cdot p_{C^{\mathcal{E}}}(y)\ \Delta x\Delta y$

where $x^{\max}$ and $y^{\max}$ are fixed in the simulations such as $p_{C^{\mathcal{D}}}(x)$ and $p_{C^{\mathcal{E}}}(y)$ are negligible for $x>x^{\max}$ and $y>y^{\max}$.

Δx and Δy are the steps which determine the precision of this approximation.

end

$\rho_k^{(i^D,i^E)}=\arg\min_\rho f(\rho)$

$J_k^{(i^D,i^E)}=\min_\rho f(\rho)$

Table III

ALGORITHM USED FOR SOLVING (30). THE FUNCTION MIN_$J_k\left(J_{k+1},\lambda_2,\overline{h},\overline{g},i^D,i^E,\gamma\right)$ SOLVES $J_k^{\lambda_1,\lambda_2}$ IN (30). IT TAKES AS PARAMETERS i^D, i^E, THE LAGRANGIAN MULTIPLIER λ_2, γ AND THE AVERAGE SNRS OF THE MAIN CHANNEL AND EAVESDROPPER CHANNEL RESPECTIVELY $\overline{h}$ AND $\overline{g}$ AND A $L_1\times L_2$ MATRIX J_{k+1}. IT RETURNS AS OUTPUT, A VALUE ρ_k AND A VALUE J_k WHICH SOLVES (30) FOR $I^{\mathcal{D}}_{k-1}=i^D$ AND $I^{\mathcal{E}}_{k-1}=i^E$.

The function min_$J_K\left(\lambda_1,\lambda_2,\overline{h},\overline{g},i^D,i^E,\gamma\right)$ solves (29) where $I^{\mathcal{D}}_{K-1}=i^D$ and $I^{\mathcal{E}}_{K-1}=i^E$

$\left[\rho_k^{(i^D,i^E)}\ \ J_k^{(i^D,i^E)}\right]$=min_$J_K\left(\lambda_1,\lambda_2,\overline{h},\overline{g},i^D,i^E,\gamma\right)$

for $\rho=0:0.01:\rho^{max}$ (ρ^{max} is arbitrary fixed during simulations)

calculate $f(\rho)=\rho+\lambda_2\cdot\left\{1-F_{C^{\mathcal{E}}}\left(\frac{1-i^E}{\rho}\right)\right\}+\lambda_1\cdot\left\{1-F_{C^{\mathcal{D}}}\left(\frac{1-i^D}{\rho}\right)\right\}$

end

$\rho_k^{(i^D,i^E)}=\arg\min_\rho f(\rho)$

$J_k^{(i^D,i^E)}=\min_\rho f(\rho)$

Table IV

ALGORITHM USED FOR SOLVING (29). THE FUNCTION MIN_$J_K\left(\lambda_1,\lambda_2,\overline{h},\overline{g},i^D,i^E,\gamma\right)$ SOLVES $J_K^{\lambda_1,\lambda_2}$ IN (29). IT TAKES AS PARAMETERS i^D, i^E, THE LAGRANGIAN MULTIPLIERS λ_1 AND λ_2, γ AND THE AVERAGE SNRS OF THE MAIN CHANNEL AND EAVESDROPPER CHANNEL RESPECTIVELY $\overline{h}$ AND $\overline{g}$. IT RETURNS AS OUTPUT, A VALUE ρ_k AND A VALUE J_k WHICH SOLVES (29) FOR $I^{\mathcal{D}}_{K-1}=i^D$ AND $I^{\mathcal{E}}_{K-1}=i^E$.

$$J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}},I_0^{\mathcal{E}}) = \min_{\rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}})} \mathbb{E}_{C_1^{\mathcal{D}},C_1^{\mathcal{E}}}\Bigg\{\rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}) + \lambda_2 \cdot \Bigg[\Bigg\{\mathbb{I}(I_0^{\mathcal{D}}<1) - \mathbb{I}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}) < 1)\Bigg\} \cdot \Bigg\{\mathbb{I}(I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}) \geq 1)\Bigg\}\Bigg] + J_2^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}), I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}))\Bigg\} \tag{31}$$

$$J_2^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}},I_1^{\mathcal{E}}) = \min_{\rho_2(I_1^{\mathcal{D}},I_1^{\mathcal{E}})} \mathbb{E}_{C_2^{\mathcal{D}},C_2^{\mathcal{E}}}\Bigg\{\rho_2(I_1^{\mathcal{D}},I_1^{\mathcal{E}}) + \lambda_2 \cdot \Bigg[\Bigg\{\mathbb{I}(I_1^{\mathcal{D}}<1) - \mathbb{I}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2(I_1^{\mathcal{D}},I_1^{\mathcal{E}}) < 1)\Bigg\} \cdot \Bigg\{\mathbb{I}(I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2(I_1^{\mathcal{D}},I_1^{\mathcal{E}}) \geq 1)\Bigg\}\Bigg] + J_3^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2(I_1^{\mathcal{D}},I_1^{\mathcal{E}}), I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2(I_1^{\mathcal{D}},I_1^{\mathcal{E}}))\Bigg\} \tag{32}$$

$$J_3^{\lambda_1,\lambda_2}(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) = \min_{\rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}})} \mathbb{E}_{C_3^{\mathcal{D}},C_3^{\mathcal{E}}}\Bigg\{\rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) + \lambda_2 \cdot \Bigg[\Bigg\{\mathbb{I}(I_2^{\mathcal{D}}<1)\Bigg\} \cdot \Bigg\{\mathbb{I}(I_2^{\mathcal{E}} + C_3^{\mathcal{E}} \cdot \rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) \geq 1)\Bigg\}\Bigg] + \lambda_1 \cdot \mathbb{I}(I_2^{\mathcal{D}} + C_3^{\mathcal{D}} \cdot \rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) < 1) \tag{33}$$

In all these equations (31), (32) and (33), we know ξ_0, ξ_s and also λ_1 and λ_2 which are fixed. We start solving these equations from the last one (33). To solve (33), we should find the optimal function $\rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}})$. From (18), we know that when $I_2^{\mathcal{D}} \geq 1$, we have $\rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) = 0$. Thus it remains to find $\rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}})$ for $I_2^{\mathcal{D}} < 1$. Consequently, we will have in (33): $\mathbb{I}(I_2^{\mathcal{D}} < 1) = 1$ because we will be interested in the case where $I_2^{\mathcal{D}} < 1$. Moreover, we observe in (33) that when $I_2^{\mathcal{E}} \geq 1$, we have $\mathbb{I}(I_2^{\mathcal{E}} + C_3^{\mathcal{E}} \cdot \rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) \geq 1) = 1$. Thus $J_3^{\lambda_1,\lambda_2}(I_2^{\mathcal{D}},I_2^{\mathcal{E}})$ will not depend on $I_2^{\mathcal{E}}$ when it is greater or equal to 1. This confirms also the choice in (18), where ρ_k does not depend on $I_{k-1}^{\mathcal{E}}$ when $I_{k-1}^{\mathcal{E}} \geq 1$. So, it is sufficient to solve (33), for $I_2^{\mathcal{E}} \leq 1$. And when $I_2^{\mathcal{E}} > 1$, we have $\rho_3(I_2^{\mathcal{D}},I_2^{\mathcal{E}}) = \rho_3(I_2^{\mathcal{D}},1)$. Using also $\mathbb{E}_{C_3^i}\Big\{\mathbb{I}(I_2^i + C_3^i \cdot \rho_3 < 1)\Big\} = F_{C^i}\Big(\frac{1-I_2^i}{\rho_3}\Big)$ where $i \in \{\mathcal{D},\mathcal{E}\}$, we can write the dynamic programming recursion as:

$$J_1^{\lambda_1,\lambda_2}(I_0^{\mathcal{D}},I_0^{\mathcal{E}}) = \min_{\rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}})} \Bigg\{\rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}) + \lambda_2 \cdot \Bigg[\Bigg\{1 - F_{C^{\mathcal{D}}}\Bigg(\frac{1-I_0^{\mathcal{D}}}{\rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}})}\Bigg)\Bigg\} \cdot \Bigg\{1 - F_{C^{\mathcal{E}}}\Bigg(\frac{1-I_0^{\mathcal{E}}}{\rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}})}\Bigg)\Bigg\}\Bigg] + \mathbb{E}_{C_1^{\mathcal{D}},C_1^{\mathcal{E}}} J_2^{\lambda_1,\lambda_2}\Bigg(I_0^{\mathcal{D}} + C_1^{\mathcal{D}} \cdot \rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}}), I_0^{\mathcal{E}} + C_1^{\mathcal{E}} \cdot \rho_1(I_0^{\mathcal{D}},I_0^{\mathcal{E}})\Bigg)\Bigg\} \tag{34}$$

$$J_2^{\lambda_1,\lambda_2}(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}) = \min_{\rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})} \left\{ \rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}) + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{D}}} \left(\frac{1 - I_1^{\mathcal{D}}}{\rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})} \right) \right\} \cdot \left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_1^{\mathcal{E}}}{\rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})} \right) \right\} \right] + \mathbb{E}_{C_2^{\mathcal{D}}, C_2^{\mathcal{E}}} J_3^{\lambda_1,\lambda_2} \left(I_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}), I_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}}) \right) \right\} \tag{35}$$

$$J_3^{\lambda_1,\lambda_2}(I_2^{\mathcal{D}}, I_2^{\mathcal{E}}) = \min_{\rho_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})} \left\{ \rho_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}}) + \lambda_2 \cdot \left[\left\{ 1 - F_{C^{\mathcal{E}}} \left(\frac{1 - I_2^{\mathcal{E}}}{\rho_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})} \right) \right\} \right] + \lambda_1 \cdot F_{C^{\mathcal{D}}} \left(\frac{1 - I_2^{\mathcal{D}}}{\rho_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})} \right) \right\} \tag{36}$$

Now to solve (36), we vary $I_2^{\mathcal{D}}$ from 0 to 1 and $I_2^{\mathcal{E}}$ from γ to 1 (since $I_0^{\mathcal{E}} = \gamma$) and we determine ρ_3 which solve (36) for all the couples ($0 \leq I_2^{\mathcal{D}} \leq 1, \gamma \leq I_2^{\mathcal{E}} \leq 1$). The optimization in (36) is performed using exhaustive search method for each couple $(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})$. In the simulations we discretized $I_2^{\mathcal{D}}$ to L_1 points between 0 and 1 and $I_2^{\mathcal{E}}$ is discretized to L_2 points between γ and 1. Thus to solve (36), we have to solve $L_1 \cdot L_2$ one-dimensional optimization problem. We obtained a $L_1 \times L_2$ matrix $\rho_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})$ and a $L_1 \times L_2$ matrix $J_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})$ which will be used in the next step.

Now we discuss how to solve (35). Similarly to (36), the optimization in (35) is performed using exhaustive search method for each couple $(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})$ where $I_2^{\mathcal{D}}$ is discretized to L_1 points between 0 and 1 and $I_2^{\mathcal{E}}$ is discretized to L_2 points between γ and 1. Thus, let suppose $(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})$ is fixed: $I_1^{\mathcal{D}} = i_1^{\mathcal{D}}$ and $I_1^{\mathcal{E}} = i_1^{\mathcal{E}}$ and we want to optimize $\rho_2(i_1^{\mathcal{D}}, i_1^{\mathcal{E}})$. To perform this optimization we vary $\rho_2(i_1^{\mathcal{D}}, i_1^{\mathcal{E}})$ between 0 and $\rho^{\max}$ where $\rho^{\max}$ is observed and fixed during simulations, and we choose $\rho_2(i_1^{\mathcal{D}}, i_1^{\mathcal{E}})$ which solve $J_2(i_1^{\mathcal{D}}, i_1^{\mathcal{E}})$. Hence for each $0 \leq \rho_2 \leq \rho^{\max}$, we should evaluate $\mathbb{E}_{C_2^{\mathcal{D}}, C_2^{\mathcal{E}}} \left\{ J_3^{\lambda_1,\lambda_2} \left(i_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2, i_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 \right) \right\}$ in (35):

$$\mathbb{E}_{C_2^{\mathcal{D}}, C_2^{\mathcal{E}}} \left\{ J_3^{\lambda_1,\lambda_2} \left(i_1^{\mathcal{D}} + C_2^{\mathcal{D}} \cdot \rho_2, i_1^{\mathcal{E}} + C_2^{\mathcal{E}} \cdot \rho_2 \right) \right\} = \int_0^{\infty} \int_0^{\infty} J_3^{\lambda_1,\lambda_2} \left(i_1^{\mathcal{D}} + x \cdot \rho_2, i_1^{\mathcal{E}} + y \cdot \rho_2 \right) \cdot p_{C^{\mathcal{D}}}(x) \cdot p_{C^{\mathcal{E}}}(y) \; dx \; dy \tag{37}$$

where $i_1^{\mathcal{D}}$, $i_1^{\mathcal{E}}$ and ρ_2 are fixed. To evaluate (37) in the simulations we approximate it by:

$$\sum_{x=0}^{x^{\max}} \sum_{y=0}^{y^{\max}} J_3^{\lambda_1,\lambda_2} \left(i_1^{\mathcal{D}} + x \cdot \rho_2, i_1^{\mathcal{E}} + y \cdot \rho_2 \right) \cdot p_{C^{\mathcal{D}}}(x) \cdot p_{C^{\mathcal{E}}}(y) \; \Delta x \Delta y \tag{38}$$

where $x^{\max}$ and $y^{\max}$ are fixed in the simulations such as $p_{C^{\mathcal{D}}}(x)$ and $p_{C^{\mathcal{E}}}(y)$ are negligible for $x > x^{\max}$ and $y > y^{\max}$. Δx and Δy are the steps which determine the precision of this approximation. For each x and y, the value of $J_3^{\lambda_1,\lambda_2}\left(i_1^{\mathcal{D}} + x \cdot \rho_2, i_1^{\mathcal{E}} + y \cdot \rho_2\right)$ can be obtained from the matrix $J_3(I_2^{\mathcal{D}}, I_2^{\mathcal{E}})$ obtained in the previous step (when we have solved (36)). At the end of this step, we obtain the optimal $L_1 \times L_2$ matrix $\rho_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})$ and a $L_1 \times L_2$ matrix $J_2(I_1^{\mathcal{D}}, I_1^{\mathcal{E}})$ which will be used in the next step.

Now, to solve (34), we have only one one-dimensional optimization problem. This is because we know that $I_0^{\mathcal{D}} = 0$ and $I_0^{\mathcal{E}} = \gamma$. Thus at the end, we obtain a 1×1 matrix $\rho_1(I_0^{\mathcal{D}}, I_0^{\mathcal{E}})$.

In this example with $K = 3$, we showed how to determine, for a fixed λ_1 and λ_2, the optimal $\rho_k(I_{k-1}^{\mathcal{D}}, I_{k-1}^{\mathcal{E}})$ for $k = 1, 2, 3$. $\square$

By solving the DP optimization recursive process, the optimal rate-adaptation policies associated with the given λ_1 and λ_2 are derived. Since we need to calculate the outage probabilities f_0 and f_s in order to update the Lagrangian multiplier, we should calculate the joint probability distributions of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ for $k = 1, .., K$ and then use them in (19) and (21).

For each set of policies, we can find the joint probability distribution of $I_k^{\mathcal{D}}$ and $I_k^{\mathcal{E}}$ starting from $k = 1$ and going recursively up to $k = K$. Due to the independence of channels, for $k = 1$ the joint cumulative density function of $I_1^{\mathcal{D}}, I_1^{\mathcal{E}}$ is

$$F_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x, y) = \Pr\left(\rho_1 \cdot C_1^{\mathcal{D}} < x, \gamma + \rho_1 \cdot C_1^{\mathcal{E}} < y\right) = F_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right) \cdot F_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right)$$

which differentiated yields the joint pdf

$$p_{I_1^{\mathcal{D}} I_1^{\mathcal{E}}}(x, y) = \frac{1}{\rho_1} \cdot p_{C^{\mathcal{D}}}\left(\frac{x}{\rho_1}\right) \cdot \frac{1}{\rho_1} \cdot p_{C^{\mathcal{E}}}\left(\frac{y-\gamma}{\rho_1}\right) \tag{39}$$

where $p_{C^{\mathcal{D}}}$ and $p_{C^{\mathcal{E}}}$ are the probability density functions of the i.i.d random variables $C_1^{\mathcal{D}}, .., C_K^{\mathcal{D}}$ and $C_1^{\mathcal{E}}, .., C_K^{\mathcal{E}}$ respectively.

In our simulations, we determine for $k = 1, .., K$, $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x, y)$ for $0 \leq x \leq x^{\max}$ and $\gamma \leq y \leq y^{\max}$, such that we ensure $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x, y)$ is too small for $x > x^{\max}$ or $y > y^{\max}$. We discretized x from 0 to $x^{\max}$ and y from γ to $y^{\max}$ with a step equal to 0.01.

for $k > 1$, the joint cumulative density function is calculated recursively:

$$F_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x, y) = \Pr\left(I_{k-1}^{\mathcal{D}} + \rho_k \cdot C_k^{\mathcal{D}} < x, I_{k-1}^{\mathcal{E}} + \rho_k \cdot C_k^{\mathcal{E}} < y\right)$$

$$= \int_0^x \int_\gamma^y \Pr\left(I_{k-1}^{\mathcal{D}} + \rho_k \cdot C_k^{\mathcal{D}} < x, I_{k-1}^{\mathcal{E}} + \rho_k \cdot C_k^{\mathcal{E}} < y | I_{k-1}^{\mathcal{D}} = \alpha, I_{k-1}^{\mathcal{E}} = \beta \right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha, \beta)\, d\alpha\, d\beta$$

$$= \int_0^x \int_\gamma^y F_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)} \right) \cdot F_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)} \right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha, \beta)\, d\alpha\, d\beta$$

thus the joint pdf obtained by differentiating the joint cumulative density function can be calculated recursively using $p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x, y)$

$$p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x, y) = \int_0^x \int_\gamma^y \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{D}}}\left(\frac{x-\alpha}{\rho_k(\alpha,\beta)} \right) \cdot \frac{1}{\rho_k(\alpha,\beta)} \cdot p_{C^{\mathcal{E}}}\left(\frac{y-\beta}{\rho_k(\alpha,\beta)} \right) \cdot p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(\alpha, \beta)\, d\alpha\, d\beta \tag{40}$$

In the case where $\rho_k(x, y) = 0$ we have $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x, y) = p_{I_{k-1}^{\mathcal{D}} I_{k-1}^{\mathcal{E}}}(x, y)$. All the integrals are approximated using the rectangular method.

When we obtain the optimal values of λ_1 and λ_2, which verify the constraints, we can calculate the secrecy throughput (20) using $p_{I_k^{\mathcal{D}} I_k^{\mathcal{E}}}(x, y)$ and $\rho_k(x, y)$. We recall that this "optimal" throughput is obtained for an arbitrary fixed $\gamma \in [0, 1]$. Now we discuss the choice of γ. In the simulations, we observe that the secrecy throughput increases when γ increases, however it is difficult or impossible to satisfy the outage probabilities constraints for high values of γ i.e. the Lagrangian multipliers does not converge to satisfy the constraints. Thus we will be interested to find the maximum value of γ which can verify the outage probabilities constraints.

VI. Numerical Results

In our numerical examples, the parameter settings are as follows: $\overline{h} = 15$ dB, $\overline{g} = 5$ dB, $\xi_\epsilon = 10^{-3}$ and $\xi_s = 10^{-3}$.

The simulations are done for several values of K, the maximum number of transmissions.

In Fig.2, we show the secrecy throughput η vs the maximum number of transmissions K using the "INR scheme" described in [4] (see Fig.7 in [4]) and the new "adaptive INR scheme" described in this paper. The results show that an important gain is obtained using the new scheme when $K > 3$. However, when K is small eg. for K=1 or 3, the secrecy throughput η stills negligible using the new scheme due to insufficient diversity.

VII. Conclusion

In this paper, we considered the reliable and secure communication over block-fading wiretap channels when the transmitter has no instantaneous channel state information. The truncated

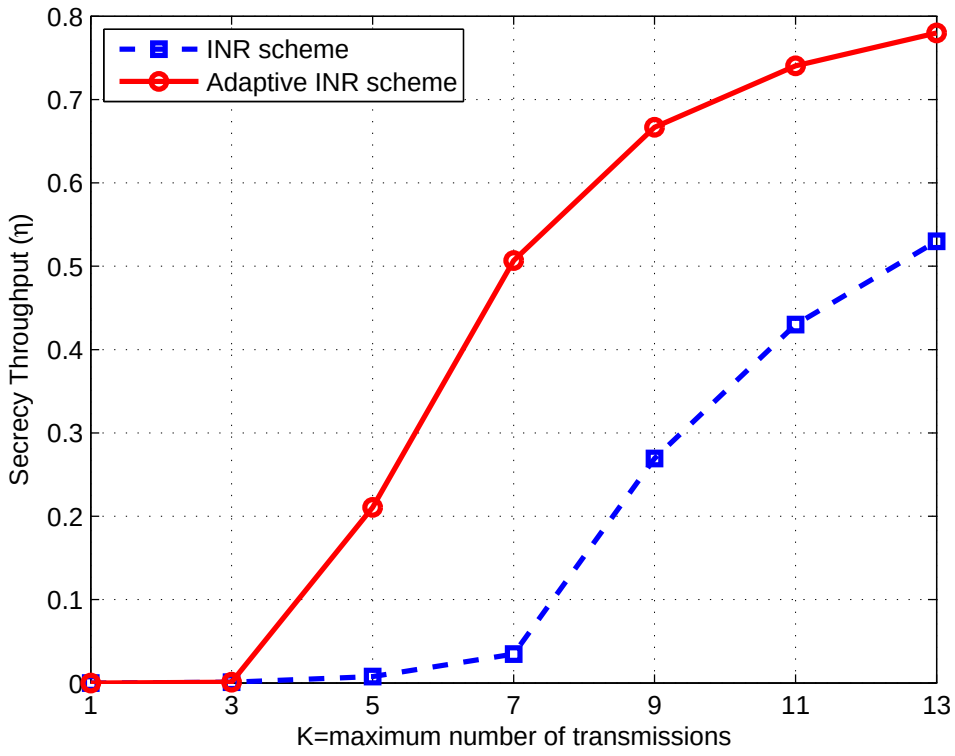

Figure 2. Secrecy throughput η vs the maximum number of transmissions K under a target secrecy outage probability $\xi_s = 10^{-3}$ and a target connection outage probability $\xi_\epsilon = 10^{-3}$, when the main and the eavesdropper channel average SNRs are 15 and 5 dB respectively.

HARQ (limited number of transmission attempts) was considered here and we used dynamic programming to find the optimal rate adaptation policy to optimize the secrecy throughput of the outage-constrained transmission. We show that the proposed rate-adaptive HARQ scheme has a significant improvement in terms of secrecy throughput compared to non-adaptive fixed-rate HARQ.

REFERENCES

[1] G. Caire and D. Tuninetti, "The throughput of hybrid-arq protocols for the gaussian collision channel," *IEEE Trans. Inf. Theor.*, vol. 47, no. 5, pp. 1971–1988, July 2001.

[2] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-arq protocols for gaussian block-fading channels," *IEEE Trans. Inf. Theor.*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[5] L. Szczecinski, S. Khosravirad, P. Duhamel, and M. Rahman, "Rate allocation and adaptation for incremental redundancy truncated harq," *IEEE Trans. Comm.*, vol. 99, pp. 1–11, 2013.

[6] L. Szczecinski, C. Correa, and L. Ahumada. Variable-rate retransmissions for incremental redundancy hybrid arq. [Online]. Available: http://arxiv.org/abs/1207.0229

[7] S. R. Khosravirad, L. Szczecinski, and F. Labeau, "Rate-adaptive harq in relay-based cooperative transmission," in *ICC*, 2013.

[8] M. Zorzi and R. R. Rao, "On the use of renewal theory in the analysis of arq protocols," *IEEE Trans. Commun.*, vol. 44, no. 9, pp. 1077–1081, Sep. 1996.

Bibliographie

[1] Zeina Mheich, Florence Alberge, and Pierre Duhamel. Achievable rates optimization for broadcast channels using finite size constellations under transmission constraints. *EURASIP Journal on Wireless Communications and Networking*, 2013(1) :254, 2013.

[2] Americo Correia, Nuno Souto, Armando Soares, Rui Dinis, and Joao Silva. Multiresolution with hierarchical modulations for long term evolution of umts. *EURASIP Journal on Wireless Communications and Networking*, 2009(1) :240140, 2009.

[3] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27 :379–423, 623–656, July, October 1948.

[4] Cisco. Cisco visual networking index : Global mobile data traffic forecast update, 2010-2015, 2011. White paper.

[5] T. M. Cover. Broadcast channels. *IEEE Trans.on Inform.Theory*, 18 :2–14, 1972.

[6] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, Second Edition, 2006.

[7] A. D. Wyner. The wiretap channel. *Bell System Technical Journal*, 54 :1355–1387, 1975.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman. The gaussian wiretap channel. *IEEE trans. Inf. Theory*, 24(4) :451–456, 1978.

[9] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE trans. Inf. Theory*, 24(3) :339–348, 1978.

[10] J. Barros and M. R D Rodrigues. Secrecy capacity of wireless channels. In *Information Theory, 2006 IEEE International Symposium on*, pages 356–360, 2006.

[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Secure communication over fading channels. *IEEE trans. Inf. Theory*, 54(6) :2470–2492, 2008.

[12] P. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE trans. Inf. Theory*, 54(10) :4687–4698, 2008.

[13] Ruoheng Liu, Tie Liu, H.V. Poor, and S. Shamai. New results on multiple-input multiple-output broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 59(3) :1346–1359, 2013.

[14] Jiangyuan Li and A.P. Petropulu. On ergodic secrecy rate for gaussian MISO wiretap channels. *Wireless Communications, IEEE Transactions on*, 10(4) :1176–1187, April 2011.

[15] Yingbin Liang and H.V. Poor. Multiple-access channels with confidential messages. *Information Theory, IEEE Transactions on*, 54(3) :976–1002, 2008.

[16] Ruoheng Liu, I. Maric, R.D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *Information Theory, 2006 IEEE International Symposium on*, pages 957–961, 2006.

[17] E. Tekin and A. Yener. The gaussian multiple access wire-tap channel with collective secrecy constraints. In *Information Theory, 2006 IEEE International Symposium on*, pages 1164–1168, 2006.

[18] Xiaojun Tang, Ruoheng Liu, Predrag Spasojević, and H. Vincent Poor. Multiple access channels with generalized feedback and confidential messages. In *In IEEE Inf. Theory Workshop on Frontiers in Coding Theory*, 2007.

[19] Ruoheng Liu, I. Maric, P. Spasojevic, and R.D. Yates. Discrete memoryless interference and broadcast channels with confidential messages : Secrecy rate regions. *Information Theory, IEEE Transactions on*, 54(6) :2493–2507, 2008.

[20] Yingbin Liang, A. Somekh-Baruch, H.V. Poor, S. Shamai, and S. Verdu. Capacity of cognitive interference channels with and without secrecy. *Information Theory, IEEE Transactions on*, 55(2) :604–619, 2009.

[21] P. P. Bergmans. Random coding theorem for broadcast channels with degraded components. *IEEE Trans. on Inform. Theory*, 19(2), 1973.

[22] P. P. Bergmans. A simple converse for broadcast channels with additive white gaussian noise. *IEEE Trans. on Inform. Theory*, 20 :279–280, March 1974.

[23] European telecommunications standards institute, digital video broadcasting (dvb), framing structure, channel coding and modulation for digital terrestrial television, etsi en 300 744.

[24] European telecommunications standards institute, "digital video broadcasting (dvb), system specifications for satellite services to handheld devices (sh) below 3 ghz" etsi ts 102 585.

[25] Y. Liu and C. Heneghan. Optimization of hierarchical modulation for use of scalable media. *EURASIP j. advances signal processing, 2010*, 2010.

[26] A. R. Calderbank and L. H. Ozarow. Nonequiprobable signaling on the gaussian channel. *IEEE Trans. on Inform. Theory*, 36(4) :726–740, July 1990.

[27] D. Sommer and G. Fettweis. Shaping by non-uniform qam for awgn channels and applications using turbo coding. In *ITG Conference Source and Channel Coding*, pages 81–86, January 2000.

[28] Xiaoqing Wang, Jian Fu, Xiaoqing Wang, Changyong Pan, and Zhixing Yang. Shaping gain for awgn channel by non-uniform constellation in ldpc-coded system. In *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, pages 1302–1306, 2008.

[29] T. Arafa, W. Sauer-Greff, and R. Urbansky. Performance of combined constellation shaping and bit interleaved coded modulation with iterative decoding (bicm-id). *Advances in Radio Science*, 9 :195–201, 2011.

[30] C. Fragouli, R. D. Wesel, D. Sommer, and G. P. Fettweis. Turbo codes with non-uniform constellations. In *Proc. IEEE Int. Conf. Communications*, 2001.

[31] X. Ma N. Varnica and A. Kavcic. Capacity of power constrained memoryless awgn channels with fixed input constellations. In *GLOBECOM*, volume 2, pages 1339–1343, Nov. 2002.

[32] D. Raphaeli and A. Gurevitz. Constellation shaping for pragmatic turbo-coded modulation with high spectral efficiency. *IEEE Trans. on Commun.*, 52(3) :341–345, March 2004.

[33] S. Y. LeGoff, B. K. Khoo, C. C. Tsimenidis, and B. S. Sharif. Constellation shaping for bandwidth-efficient turbo-coded modulation with iterative receiver. *IEEE Transactions on Wireless Communications*, 6(6) :2223–2233, June 2007.

[34] N. H. Ngo, S. A. Barbulescu, and S. S. Pietrobon. Performance of nonuniform m-ary qam constellation on nonlinear channels. In *Australian Communications Theory Workshop*, Australia, 2005.

[35] Jiayin Zhang, Dageng Chen, and Yi Wang. A new constellation shaping method and its performance evaluation in bicm-id. In *Vehicular Technology Conference Fall (VTC 2009-Fall)*, sept 2009.

[36] M.C. Valenti and Xingyu Xiang. Constellation shaping for bit-interleaved ldpc coded apsk. *IEEE Transactions on Communications*, 60(10) :2960–2970, 2012.

[37] C. Huppert and M. Bossert. On achievable rates in the two user awgn broadcast channel with finite input alphabets. In *ISIT*, Nice, France, June 2007.

[38] G. D. Raghava and B. S. Rajan. Secrecy capacity of the gaussian wiretap channel with finite complex constellation input, 2010.

[39] F. Renna, N. Laurenti, and H. V. Poor. Achievable secrecy rates for wiretap ofdm with qam constellations. In *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools, VALUETOOLS '11*, Paris, France, 2011.

[40] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch. On gaussian wiretap channels with m-pam inputs. In *Wireless Conference (EW), 2010 European*, pages 774–781, 2010.

[41] S. Bashar, Z. Ding, and C. Xiao. On secrecy rate analysis of mimo wiretap channels driven by finite-alphabet input. *IEEE Trans. on communications*, 60(12), dec. 2012.

[42] S. Bashar, Zhi Ding, and Chengshan Xiao. On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input. *Communications Letters, IEEE*, 15(5) :527–529, May 2011.

[43] Haohao Qin, Yin Sun, Tsung-Hui Chang, Xiang Chen, Chong-Yung Chi, Ming Zhao, and Jing Wang. Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs. *Wireless Communications, IEEE Transactions on*, 12(6) :2717–2729, June 2013.

[44] M. Zorzi and R R. Rao. On the use of renewal theory in the analysis of arq protocols. *IEEE Trans. Commun.*, 44(9) :1077–1081, Sep. 1996.

[45] G. Caire and D. Tuninetti. The throughput of hybrid-arq protocols for the gaussian collision channel. *IEEE Trans. Inf. Theor.*, 47(5) :1971–1988, July 2001.

[46] T.T. Kim and M. Skoglund. On the expected rate of slowly fading channels with quantized side information. *Communications, IEEE Transactions on*, 55(4) :820–829, 2007.

[47] Peng Wu and Nihar Jindal. Performance of hybrid-arq in block-fading channels : a fixed outage probability analysis. *Trans. Comm.*, 58(4) :1129–1141, April 2010.

[48] Xiaojun Tang, Ruoheng Liu, Predrag Spasojevic, and H. Vincent Poor. On the throughput of secure hybrid-arq protocols for gaussian block-fading channels. *IEEE Trans. Inf. Theor.*, 55(4) :1575–1591, April 2009.

[49] Zeina Mheich, Marie-Line Alberi Morel, and Pierre Duhamel. Optimization of unicast services transmission for broadcast channels in practical situations. *Bell Labs Technical Journal*, 17(1) :5–23, 2012.

[50] Zeina Mheich, Pierre Duhamel, Leszek Szczecinski, and Marie-Line Alberi Morel. Constellation shaping for broadcast channels in practical situations. In *Proceedings of the 19th European Signal Processing Conference (EUSIPCO 2011)*, Barcelona, 29 Aug-2 Sept. 2011.

[51] Zeina Mheich, Florence Alberge, and Pierre Duhamel. On the efficiency of transmission strategies for broadcast channels using finite size constellations. In *Proceedings of the 21st European Signal Processing Conference (EUSIPCO 2013)*, Marrakech, 9-13 Sept. 2013.

[52] Zeina Mheich, Florence Alberge, and Pierre Duhamel. The impact of finite-alphabet input on the secrecy-achievable rates for broadcast channel with confidential message. In *2014 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2014)*, Florence, Italy, May 2014.

[53] Z. Mheich, M. Le Treust, F. Alberge, P. Duhamel, and L. Szczecinski. Rate-adaptive secure HARQ protocol for block-fading channels. 2014. soumis à 22nd European Signal Processing Conference (EUSIPCO 2014).

[54] Zeina Mheich, Florence Alberge, and Pierre Duhamel. Secrecy-achievable rates for the broadcast channel with confidential message and finite constellation inputs. 2014. soumis à IEEE trans. on comm.

[55] GH. Imai and S. Hirakawa. A new multilevel coding method using error correcting codes. *IEEE Trans. on Inform. Theory*, 23 :371–377, 1977.

[56] G. Ungerboeck. Channel coding with multilevel/phase signals. *IEEE Trans. on Inform. Theory*, 28 :55–67, 1982.

[57] T M Cover. Comments on broadcast channels. *IEEE Trans. on Inform. Theory*, 44(6), october 1998.

[58] R. G. Gallager. Capacity and coding for degraded broadcast channels. *Probl. Infor. Transm.*, pages 185–193, 1974.

[59] J. Korner and K. Marton. Comparison of two noisy channels. pages 411–423, 1977.

[60] M. Bloch and J. Barros. *Physical layer security : from information theory to security engineering*. Cambridge University Press, 2011.

[61] J. Gledhill, P. Macavock, and R. Miles. Dvb-t : Hierarchical modulation. DVB, march 2000.

[62] A. Schertz and C. Weck. Hierarchical modulation-the transmission of two independent dvb-t multiplexes on a single frequency. EBU Techn., April 2003.

[63] H. Meric, J. Lacan, C. Amiot-Bazile, F. Arnal, and M-L. Boucheret. Generic approach for hierarchical modulation performance analysis : Application to dvb-sh. In *Wireless Telecommunications Symposium*, New York, USA, 2011.

[64] Vaibhav Singh. On superposition coding for wireless broadcast channels. Master's thesis, Royal Institute of Technology, Sweden, 2005.

[65] K. Yasui and T. Matsushima. Toward computing the capacity region of degraded broadcast channel. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 570–574, June 2010.

[66] R. E. Blahut. Computation of channel capacity and rate-distortion functions. *IEEE Trans. on Inform. Theory*, 18(4), July 1972.

[67] K. Yasui, T. Suko, and T. Matsushima. An algorithm for computing the secrecy capacity of broadcast channels with confidential messages. In *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pages 936–940.

[68] M. van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 43(2) :712–714, 1997.

[69] K.R. Gowtham and A. Thangaraj. Computation of secrecy capacity for more-capable channel pairs. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 529–533, July 2008.

[70] E. Calvo, D. P. Palomar, J. R. Fonollosa, and J. Vidal. The computation of the capacity region of the discrete degraded bc is a nonconvex dc problem. In *IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Canada, July 2008.

[71] J. Hagenauer. Rate-compatible punctured convolutional codes (rcpc codes) and their applications. *Communications, IEEE Transactions on*, 36(4) :389–400, 1988.

[72] C.F. Leanderson and G. Caire. The performance of incremental redundancy schemes based on convolutional codes in the block-fading gaussian collision channel. *Wireless Communications, IEEE Transactions on*, 3(3) :843–854, 2004.

[73] K.R. Narayanan and G.L. Stuber. A novel arq technique using the turbo coding principle. *Communications Letters, IEEE*, 1(2) :49–51, 1997.

[74] S. Sesia, G. Caire, and G. Vivier. Incremental redundancy hybrid arq schemes based on low-density parity-check codes. *Communications, IEEE Transactions on*, 52(8) :1311–1321, 2004.

[75] Emina Soljanin, Nedeljko Varnica, and Philip Whiting. Incremental redundancy hybrid arq with ldpc and raptor codes," submitted to. *IEEE Trans. Inf. Theory*, 2005.

[76] D. Tuninetti and G. Caire. The throughput of some wireless multiaccess systems. *Information Theory, IEEE Transactions on*, 48(10) :2773–2785, 2002.

[77] Leszek Szczecinski, S. Khosravirad, Pierre Duhamel, and M. Rahman. Rate allocation and adaptation for incremental redundancy truncated harq. *IEEE Trans. Comm.*, 61(6) :2580–2590, June 2013.

[78] Leszek Szczecinski, Ciro Correa, and Luciano Ahumada. Variable-rate retransmissions for incremental redundancy hybrid arq.

[79] S. Reza Khosravirad, Leszek Szczecinski, and Fabrice Labeau. Rate-adaptive harq in relay-based cooperative transmission. In *ICC*, 2013.

[80] Ezio Biglieri, J. Proakis, and S. Shamai. Fading channels : information-theoretic and communications aspects. *Information Theory, IEEE Transactions on*, 44(6) :2619–2692, 1998.

[81] S.Y. Le Goff, Boon Kien Khoo, C.C. Tsimenidis, and B.S. Sharif. Constellation shaping for bandwidth-efficient turbo-coded modulation with iterative receiver. *Wireless Communications, IEEE Transactions on*, 6(6) :2223–2233, 2007.

[82] T. Ghanim and M.C. Valenti. The throughput of hybrid-arq in block fading under modulation constraints. In *Information Sciences and Systems, 2006 40th Annual Conference on*, pages 253–258, 2006.

[83] Biao He and Xiangyun Zhou. Secure on-off transmission design with channel estimation errors. *Information Forensics and Security, IEEE Transactions on*, 8(12) :1923–1936, Dec 2013.

[84] L. H. Ozarow and A. D. Wyner. Wire-tap channel ii. *AT&T Bell Laboratories Technical Journal*, 63(10) :2135–2157, 1984.

[85] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, and J. M Merolla. Applications of ldpc codes to the wiretap channel. *Information Theory, IEEE Transactions on*, 53(8) :2933–2945, 2007.

[86] Ruoheng Liu, Yingbin Liang, H.V. Poor, and P. Spasojevic. Secure nested codes for type ii wiretap channels. In *Information Theory Workshop, 2007. ITW '07. IEEE*, pages 337–342, 2007.